Available online at www.sciencedirect.com
ScienceDirect
Journal of Number Theory 128 (2008) 954–978
JOURNAL OF Number Theory
www.elsevier.com/locate/jnt

On realizable Galois module classes and Steinitz classes of nonabelian extensions

Clement Bruche, Bouchaïb Sodaïgui *

Université de Valenciennes, Département de Mathématiques, Le Mont Houy, 59313 Valenciennes Cedex 9, France

Received 20 October 2006; revised 6 February 2007

Available online 24 May 2007

Communicated by David Goss

Abstract

Let k be a number field and O_k its ring of integers. Let Γ be a finite group, N/k a Galois extension with Galois group isomorphic to Γ, and O_N the ring of integers of N. Let $\mathcal{M}$ be a maximal O_k-order in the semisimple algebra $k[\Gamma]$ containing $O_k[\Gamma]$, and $\mathrm{Cl}(\mathcal{M})$ its locally free class group. When N/k is tame (i.e., at most tamely ramified), extension of scalars allows us to assign to O_N the class of $\mathcal{M}\otimes_{O_k[\Gamma]} O_N$, denoted $[\mathcal{M}\otimes_{O_k[\Gamma]} O_N]$, in $\mathrm{Cl}(\mathcal{M})$. We define the set $\mathcal{R}(\mathcal{M})$ of realizable classes to be the set of classes $c\in\mathrm{Cl}(\mathcal{M})$ such that there exists a Galois extension N/k which is tame, with Galois group isomorphic to Γ, and for which $[\mathcal{M}\otimes_{O_k[\Gamma]} O_N]=c$. Let p be an odd prime number and let ξ_p be a primitive pth root of unity. In the present article, we prove, by means of a fairly explicit description, that $\mathcal{R}(\mathcal{M})$ is a subgroup of $\mathrm{Cl}(\mathcal{M})$ when $\xi_p\in k$ and $\Gamma = V\rtimes_\rho C$, where V is an $\mathbb{F}_p$-vector space of dimension $r\geqslant 1$, C a cyclic group of order p^r-1, and ρ a faithful representation of C in V; an example is the symmetric group S_3. In the proof, we use some properties of a cyclic code and solve an embedding problem connected with Steinitz classes. In addition, we determine the set of Steinitz classes of tame Galois extensions of k, with the above group as Galois group, and prove that it is a subgroup of the class group of k.

MSC: 11R33

Keywords: Galois module structure; Realizable classes; Steinitz classes; Maximal order; Fröhlich's Hom-description of locally free class groups; Fröhlich–Lagrange resolvent; Embedding problem; Cyclic codes; Primitive polynomials

* Corresponding author.
E-mail addresses: clement.bruche@univ-valenciennes.fr (C. Bruche), bouchaib.sodaigui@univ-valenciennes.fr (B. Sodaïgui).

0022-314X/$ – see front matter
doi:10.1016/j.jnt.2007.02.009

1. Introduction and statement of main results

Throughout this article, if K is a number field, we denote by O_K its ring of integers and $\mathrm{Cl}(K)$ its class group.

Let k be a number field and Γ a finite group. Let $\mathcal{M}$ be a maximal O_k-order in $k[\Gamma]$ containing $O_k[\Gamma]$. Let $\mathrm{Cl}(O_k[\Gamma])$ (respectively $\mathrm{Cl}(\mathcal{M})$) be the locally free class group of $O_k[\Gamma]$ (respectively $\mathcal{M}$) (see [F4, Chapter I]). We denote by $\mathcal{R}(O_k[\Gamma])$ (respectively $\mathcal{R}(\mathcal{M})$) the set of realizable classes, that is the set of classes $c \in \mathrm{Cl}(O_k[\Gamma])$ (respectively $\mathrm{Cl}(\mathcal{M})$) such that there exists a Galois extension N/k at most tamely ramified (we abbreviate this to: tame), with Galois group isomorphic to Γ and the class of O_N (respectively $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$) is equal to c; we will say that c is realizable by the extension N/k. It is easily seen that $\mathcal{R}(O_k[\Gamma]) \subset \mathrm{Cl}^\circ(O_k[\Gamma])$ (respectively $\mathcal{R}(\mathcal{M}) \subset \mathrm{Cl}^\circ(\mathcal{M})$) (see [M2, (4.4)]), where $\mathrm{Cl}^\circ(O_k[\Gamma])$ (respectively $\mathrm{Cl}^\circ(\mathcal{M})$) is the kernel of the morphism $\mathrm{Cl}(O_k[\Gamma]) \to \mathrm{Cl}(k)$ (respectively $\mathrm{Cl}(\mathcal{M}) \to \mathrm{Cl}(k)$) induced by the augmentation $O_k[\Gamma] \to O_k$ (respectively $\mathcal{M} \to O_k$). The results of McCulloh (see [M3]) lead one to the following conjecture.

Conjecture 1. *The set* $\mathcal{R}(O_k[\Gamma])$ *is a subgroup of* $\mathrm{Cl}^\circ(O_k[\Gamma])$.

A difficulty coming from local units of group rings arises when we attempt to prove this conjecture (see the proof of Fröhlich's conjecture in [T]; see [BS1,BS2]). An approach toward circumventing this difficulty is to study the following weaker conjecture.

Conjecture 2. *The set* $\mathcal{R}(\mathcal{M})$ *is a subgroup of* $\mathrm{Cl}^\circ(\mathcal{M})$.

Conjecture 1 implies Conjecture 2. Indeed: extension of scalars from $O_k[\Gamma]$ to $\mathcal{M}$ induces a surjective morphism $\mathrm{Ex} : \mathrm{Cl}(O_k[\Gamma]) \to \mathrm{Cl}(\mathcal{M})$ and it is clear that $\mathrm{Ex}(\mathcal{R}(O_k[\Gamma])) = \mathcal{R}(\mathcal{M})$.

If k is any number field and Γ is abelian, McCulloh [M3] proved Conjecture 1 by means of a "Stickelberger map."

Let A_4 be the tetrahedral group (i.e., the alternating group of degree 4) and D_4 the dihedral group of order 8. In [BS1] Conjecture 1 was proved for A_4; more precisely, the equality $\mathcal{R}(O_k[A_4]) = \mathrm{Cl}^\circ(O_k[A_4])$ was established for all number fields k. In [BS2] it is shown that $\mathcal{R}(O_k[D_4]) = \mathrm{Cl}^\circ(O_k[D_4])$ for any number field k such that the ray class group of k with modulus $4O_k$ has odd order. For previous work toward Conjecture 2, see for instance [BGS,GS2,So2, So4,So5,So6].

Let p be a prime number. Let $\mathbb{F}_p$ be the finite field of p elements, which we will often identify with $\mathbb{Z}/p\mathbb{Z}$. Let V be an $\mathbb{F}_p$-vector space of dimension $r \geqslant 1$, and C a cyclic group of order $p^r - 1$. Let

$$\rho : C \to \mathrm{Aut}_{\mathbb{F}_p}(V)$$

be a linear representation of C in V. We denote $\Gamma = V \rtimes_\rho C$ the semidirect product of V by C which is defined by ρ.

In [BGS], we consider the case: $p = 2$ and $r \geqslant 2$; under the hypothesis that ρ is faithful, we prove Conjecture 2 by means of a fairly explicit description of $\mathcal{R}(\mathcal{M})$ (see [BGS, Theorem 1.1]). A part of the present paper is to study Conjecture 2 in the situation: p odd and $r \geqslant 1$.

The Wedderburn decomposition of the semisimple algebra $k[C]$ as a product of simple algebras is (see [CR2, p. 330 and §74]):

$$k[C] \simeq \prod_{i=0}^{n} k(\chi_i),$$

where $n+1$ is the number of the conjugacy classes over k of absolutely irreducible characters of C (i.e., characters of irreducible complex representations), and for each $i \in \{0, 1, \ldots, n\}$, χ_i is a representative of one of these classes, χ_0 is the trivial character, and $k(\chi_i)$ is the extension of k obtained by adjoining to k the values of χ_i.

Let $\mathcal{M}(C)$ be the maximal O_k-order in $k[C]$. Since C is abelian, we have

$$\mathrm{Cl}\big(\mathcal{M}(C)\big) \simeq \prod_{i=0}^{n} \mathrm{Cl}\big(k(\chi_i)\big), \quad \text{and then} \quad \mathrm{Cl}^{\circ}\big(\mathcal{M}(C)\big) \simeq \prod_{i=1}^{n} \mathrm{Cl}\big(k(\chi_i)\big).$$

Let $\mathcal{R}(\mathcal{M}(C))$ be the set consisting of the classes in $\mathrm{Cl}(\mathcal{M}(C))$ which are realizable by tame Galois extensions of k, with Galois group isomorphic to C. By [M3], $\mathcal{R}(\mathcal{M}(C))$ is a subgroup of $\mathrm{Cl}^{\circ}(\mathcal{M}(C))$ which can be described by a Stickelberger map. We will often identify $\mathcal{R}(\mathcal{M}(C))$ with a subgroup of $\prod_{i=1}^{n} \mathrm{Cl}(k(\chi_i))$.

Now, suppose p odd, $r \geqslant 1$, ρ faithful and $\xi_p \in k$; where ξ_p is a primitive pth root of unity. Let $\mathcal{M}$ be a maximal O_k-order in $k[\Gamma]$ which contains $O_k[\Gamma]$. In Section 4, we will determine the conjugacy classes over k of the absolutely irreducible characters of Γ, and show that

$$\mathrm{Cl}^{\circ}(\mathcal{M}) \simeq \prod_{i=1}^{n} \mathrm{Cl}\big(k(\chi_i)\big) \times \mathrm{Cl}(k). \tag{1.1}$$

We will often identify $\mathrm{Cl}^{\circ}(\mathcal{M})$ with $\prod_{i=1}^{n} \mathrm{Cl}(k(\chi_i)) \times \mathrm{Cl}(k)$ under the isomorphism of (1.1).

We fix the following notation which will be in force throughout this article. If K/k is an extension of number fields, then $N_{K/k}$ denotes the norm map in K/k. If G is an abelian group and $m \in \mathbb{N}$, then G^m denotes the subgroup of the mth powers of elements of G.

In Section 4, we shall prove the following theorem.

Theorem 1.1. *Let k be a number field which contains ξ_p and $\Gamma = V \rtimes_{\rho} C$, where p is an odd prime number. Suppose that the representation ρ is faithful. We identify $\mathrm{Cl}^{\circ}(\mathcal{M})$ with $\prod_{i=1}^{n} \mathrm{Cl}(k(\chi_i)) \times \mathrm{Cl}(k)$. Then $\mathcal{R}(\mathcal{M})$ is a subgroup of $\mathrm{Cl}^{\circ}(\mathcal{M})$, equal to the following subgroup A:*

$$A = \left\{ \left(c_1, c_2, \ldots, c_n, x \prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i) \right) \;\middle|\; (c_1, c_2, \ldots, c_n) \in \mathcal{R}\big(\mathcal{M}(C)\big),\ x \in \mathrm{Cl}(k)^{p^{r-1}(p-1)/2} \right\}.$$

Remark. An immediate consequence of Theorem 1.1 is: $\mathcal{R}(\mathcal{M})$ is isomorphic to the group $\mathcal{R}(\mathcal{M}(C)) \times \mathrm{Cl}(k)^{p^{r-1}(p-1)/2}$.

We will see in Section 2 that the symmetric group S_3 is an example of a group Γ which satisfies the hypotheses of Theorem 1.1 (see Remark 2 which follows Proposition 2.3, in this case $p = 3$ and $r = 1$).

Corollary 1.2. *Let k be any number field and $\Gamma = S_3$. Then $\mathcal{R}(\mathcal{M})$ is the subgroup* $\mathrm{Cl}^\circ(\mathcal{M})$. *In this case,* $\mathrm{Cl}(\mathcal{M}) \simeq \mathrm{Cl}(k) \times \mathrm{Cl}(k) \times \mathrm{Cl}(k)$, *and* $\mathcal{R}(\mathcal{M}) = \mathrm{Cl}(k) \times \mathrm{Cl}(k)$.

This corollary extends, without any hypothesis on the base field k, the following main result of [So2] in the case of the metacyclic group S_3 (see §4, Proof of Corollary 1.2): if $\xi_3 \notin k$, then $\mathcal{R}(\mathcal{M}) = \mathrm{Cl}(k) \times \mathrm{Cl}(k)$.

Now, recall the definition of Steinitz class. Let M be a finitely generated, torsion-free module of rank s over O_k. Then, there exists an ideal I of O_k such that $M \simeq O_k^{s-1} \oplus I$ as an O_k-module. The class of I in $\mathrm{Cl}(k)$ is called the Steinitz class of M, and will be denoted by $\mathrm{cl}_k(M)$ (see [FT, Theorem 13, p. 95], or [Co2, Theorem 1.2.19, p. 9 and Corollary 1.2.24, p. 11]). The structure of M as an O_k-module is determined up to isomorphism by its rank and its Steinitz class. One applies the previous discussion to $M = O_K$, where K/k is an extension of number fields of degree s; we will also say that $\mathrm{cl}_k(O_K)$ is the Steinitz class of K/k.

As we have seen for instance in [BGS,GS2,So4,So5], when we attempt to study Conjecture 2, we are faced with the embedding problem connected with the problem of studying Steinitz classes.

Another part of the present paper is to study the Steinitz classes in the following setting.

Let Γ be a finite group and Δ a normal subgroup of Γ. We have the following exact sequence:

$$\Sigma : 1 \to \Delta \to \Gamma \to \Gamma/\Delta \to 1.$$

We fix a tame Galois extension E/k with Galois group isomorphic to Γ/Δ. We denote by $R_t(E/k, \Sigma)$ (t means tame) the set of (realizable) classes $c \in \mathrm{Cl}(k)$ satisfying: there exists a tame Galois extension N/k whose Galois group is isomorphic to Γ and whose Steinitz class is equal to c, containing E, with an isomorphism π from $\mathrm{Gal}(N/k)$ to Γ such that E is the subfield of N fixed by $\pi^{-1}(\Delta)$, and the action of Γ on E corresponds via π to the prescribed action of Γ/Δ on E.

If $\Delta = \Gamma$, then $R_t(E/k, \Sigma)$ is simply the set of the Steinitz classes of tame Galois extensions of k whose Galois group is isomorphic to Γ; we write $R_t(k, \Gamma)$ instead of $R_t(E/k, \Sigma)$.

As we have seen in [BGS, §1], the trivial injection $1 \to \Gamma$ induces the restriction morphism $\mathrm{res}_1^\Gamma : \mathrm{Cl}(O_k[\Gamma]) \to \mathrm{Cl}(k)$, and we have $\mathrm{res}_1^\Gamma(\mathcal{R}(O_k[\Gamma])) = R_t(k, \Gamma)$. Thus Conjecture 1 implies the following conjecture.

Conjecture 3. *The set $R_t(k, \Gamma)$ is a subgroup of* $\mathrm{Cl}(k)$.

As a consequence of [M3], this conjecture is true when Γ is abelian. When Γ is not abelian, for recent works toward the study of $R_t(E/k, \Sigma)$ and Conjecture 3, see for instance [BGS,C, GS1,GS3,So3,So5,Sov].

In the present article, we are interested in the case where $\Gamma = V \rtimes_\rho C$ and $\Delta = V$. We have $\mathrm{Gal}(E/k) \simeq C$, therefore E/k is a cyclic extension of degree $p^r - 1$. In [BGS], we treat the case: $p = 2$, $r \geqslant 2$; assuming ρ faithful, we determine $R_t(E/k, \Sigma)$ and prove Conjecture 3 for any number field (see [BGS, Theorem 1.4]). In this paper we treat the situation: p odd and $r \geqslant 1$.

By [M3], the set $R_t(k, C)$ of Steinitz classes of tame Galois extensions of k, whose Galois group is isomorphic to C, is a subgroup of $\mathrm{Cl}(k)$.

In Section 3, we will prove the following result.

Theorem 1.3. *Let $\Gamma = V \rtimes_\rho C$. Assume p odd, $r \geqslant 1$ and the representation ρ faithful. Let k be a number field and E/k a tame cyclic extension of degree $p^r - 1$.*

(i) *If $\xi_p \in E$, then $R_t(E/k, \Sigma) = \mathrm{cl}_k(O_E)^{p^r}(N_{E/k}(\mathrm{Cl}(E)))^{p^{r-1}(p^r-1)(p-1)/2}$.*
(ii) *Suppose $\xi_p \in k$, then $R_t(k, \Gamma)$ is a subgroup of $\mathrm{Cl}(k)$ and*

$$R_t(k, \Gamma) = R_t(k, C)^{p^r}\big(\mathrm{Cl}(k)\big)^{p^{r-1}(p^r-1)(p-1)/2},$$

where $R_t(k, C)$ is the group of Steinitz classes of tame Galois extensions of k whose Galois group is isomorphic to C.

Corollary 1.4. *With the notation and hypotheses of Theorem* 1.3*, we have the following assertions*:

(i) *If $\xi_p \in E$ and O_E is a free O_k-module, then $R_t(E/k, \Sigma)$ is the subgroup $N_{E/k}(\mathrm{Cl}(E))^{p^{r-1}(p^r-1)(p-1)/2}$ of $\mathrm{Cl}(k)$.*
(ii) *Assume that $\xi_p \in k$. If k contains a primitive $(p^r - 1)$th root of unity ξ_{p^r-1}, then $R_t(k, \Gamma) = \mathrm{Cl}(k)^{p^{r-1}}$. In particular, $R_t(k, S_3) = \mathrm{Cl}(k)$.*

Finally, we point out that the present article originates from an attempt to extend the results and arguments of [BGS]. For the reader's convenience (especially the non-French-speaking reader), we will try to give sufficient details for some proofs and definitions which are analogous to those in [BGS], in order to help the reader to understand the similarities and differences between [BGS] and this paper.

2. Preliminaries

From now on and throughout the present paper, p is an odd prime number and $r \geqslant 1$.

Let V be an $\mathbb{F}_p$-vector space of dimension r, and G an abelian group with order relatively prime to p. (Then $\mathbb{F}_p[G]$ is a semisimple algebra.) Let

$$\rho : G \to \mathrm{Aut}_{\mathbb{F}_p}(V)$$

be a linear representation of G in V. We denote by $\Gamma = V \rtimes_\rho G$ the semidirect product of V by G which is defined by ρ.

If $g \in G$ and $v \in V$, we set $gv = \rho(g)(v)$; this defines on V a natural structure of $\mathbb{F}_p[G]$-module.

In the sequel, in order to simplify the notation, one identifies groups which are isomorphic whenever we can do so without any ambiguity; for instance we will very often consider G and V as subgroups of Γ.

Let E be a number field which contains ξ_p and let $E^\times = E \setminus \{0\}$. By Kummer theory (see for instance [Co2, §10.2]), an extension N/E is Galois with Galois group V if and only if there exists

a subspace W of the $\mathbb{F}_p$-vector space $E^\times/E^{\times p}$ having dimension r, such that $N = E(\sqrt[p]{W})$, where $\sqrt[p]{W}$ is the set of all pth roots of the elements of $E^\times$ belonging to the classes of W, and such that the following pairing is perfect:

$$\begin{aligned}\langle,\rangle : V \times W &\to \langle\xi_p\rangle,\\ (v, w) &\mapsto \langle v, w\rangle = v\big(\sqrt[p]{w}\big)/\sqrt[p]{w},\end{aligned}$$

where $\sqrt[p]{w}$ is an abuse of notation for a chosen pth root of a chosen representative of the class w, and $\langle\xi_p\rangle$ is the group of the pth roots of unity.

The group $\langle\xi_p\rangle$ being isomorphic to $\mathbb{F}_p$ as an $\mathbb{F}_p$-vector space, the preceding pairing may be considered as a nondegenerate $\mathbb{F}_p$-bilinear form from $V \times W$ to $\mathbb{F}_p$. Then, the vector spaces V and W are dual:

$$W \simeq \mathrm{Hom}\big(V, \langle\xi_p\rangle\big) \simeq \mathrm{Hom}_{\mathbb{F}_p}(V, \mathbb{F}_p).$$

Hence, there exists a unique linear representation

$$\rho^* : G \to \mathrm{Aut}_{\mathbb{F}_p}(W)$$

such that for all $g \in G$, $v \in V$, $w \in W$,

$$\big\langle \rho(g)(v), \rho^*(g)(w)\big\rangle = \langle v, w\rangle,$$

which is equivalent to $\langle \rho(g^{-1})(v), w\rangle = \langle v, \rho^*(g)(w)\rangle$.

The representation ρ^* is called the contragredient representation of ρ (see [CR1, §10D, p. 245]). Therefore the vector space W is equipped with the $\mathbb{F}_p[G]$-module structure defined by: for all $g \in G$, $gw = \rho^*(g)(w)$.

If E/k is a Galois extension with Galois group G, then any $g \in G$ induces an automorphism of the $\mathbb{F}_p$-vector space $E^\times/E^{\times p}$, which will also be denoted by g. Hence, the $\mathbb{F}_p$-vector space $E^\times/E^{\times p}$ has a natural $\mathbb{F}_p[G]$-module structure.

Arguing as in the proof of [BGS, Proposition 2.1, p. 8], we obtain the following proposition.

Proposition 2.1. *Let k be a number field, E/k a Galois extension containing ξ_p with $\mathrm{Gal}(E/k) = G$, W an $\mathbb{F}_p$-subspace of $E^\times/E^{\times p}$ and $N = E(\sqrt[p]{W})/E$ a Galois extension with $\mathrm{Gal}(N/E) = V$. Then the following assertions are equivalent*:

(i) *N/k is Galois with $\mathrm{Gal}(N/k) \simeq \Gamma = V \rtimes_\rho G$.*
(ii) *The space W is stable under the action of G and the corresponding natural representation from G to $\mathrm{Aut}_{\mathbb{F}_p}(W)$ is the contragredient ρ^* of ρ.*

From now on and throughout the present article, we assume that $G = C$ is a cyclic group of order $p^r - 1$. We choose a generator σ of C.

Let $\overline{\mathbb{F}}_p$ be an algebraic closure of $\mathbb{F}_p$. In what follows, the extensions of $\mathbb{F}_p$ are assumed to be included in $\overline{\mathbb{F}}_p$.

The following terminology comes from coding theory (see for instance [Ro, p. 293]).

Definition 2.2. Let $f \in \mathbb{F}_p[X]$ of degree $n \geqslant 1$. We say that f is primitive if it is the minimal polynomial of a generator of the cyclic group $\mathbb{F}_{p^n}^{\times}$ $(= \mathbb{F}_{p^n} \setminus \{0\})$.

Examples. There exist tables for primitive polynomials, see for instance [Ro, pp. 459–463] and [LN, Chapter 10, Tables E and F, pp. 564–566]. Table E of [LN] lists all primitive polynomials of degree 2 for $11 \leqslant p \leqslant 31$, and Table F lists one primitive polynomial of degree n for all $n \geqslant 2$ and $p < 50$ such that $p^n < 10^9$. Let us give one for some values of n and p:

$$\begin{aligned}
&n = 1,\ p = 3\colon\ X + 1; && n = 2,\quad p = 5\colon\ X^2 + X + 2;\\
&n = 3,\ p = 7\colon\ X^3 + X^2 + X + 2; && n = 4,\quad p = 11\colon\ X^4 + X + 2;\\
&n = 5,\ p = 13\colon\ X^5 + X^3 + X + 11; && n = 6,\quad p = 23\colon\ X^6 + X^5 + 7;\\
&n = 5,\ p = 47\colon\ X^5 + X + 42; && n = 18,\ p = 3\colon\ X^{18} + X^5 + 2.
\end{aligned}$$

Remarks. (1) The roots of an irreducible polynomial of $\mathbb{F}_p[X]$ of degree n have the same order in $\mathbb{F}_{p^n}^{\times}$, because they are conjugate under the Frobenius of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. In particular, each root of a primitive polynomial of degree n is a generator of the group $\mathbb{F}_{p^n}^{\times}$.

(2) Computing primitive polynomials (see for instance [Ro, pp. 456–457]): Let $e = p^n - 1$. Let $\Phi_e(X)$ be the eth cyclotomic polynomial over $\mathbb{F}_p$; that is the monic polynomial whose roots in $\overline{\mathbb{F}}_p$ are (all) the primitive eth roots of unity. Then $\Phi_e(X) \in \mathbb{F}_p[X]$, and clearly the irreducible factors of $\Phi_e(X)$ are precisely the primitive polynomials of degree n. To compute ones, we can use Berlekamp's algorithm (see [Co1, §3.4, Algorithms 3.4.10 and 3.4.11, pp. 131–132]), and the formula $\Phi_e(X) = \prod_{d|e}(X^{e/d} - 1)^{\mu(d)}$ (see [Ro, Theorem A.2.4, Example A.2.3, p. 441]), where d runs through the set of positive divisors of e and μ is the Möbius function ($\mu(1) = 1$; if d is a product of m distinct primes, $\mu(d) = (-1)^m$; otherwise $\mu(d) = 0$).

A similar argument as in the proof of [BGS, Proposition 2.3, p. 10] allows us to have:

Proposition 2.3.

(1) *With the previous notation, if the representation ρ is faithful, then it is irreducible. Furthermore, the minimal polynomial of $\rho(\sigma) \in \mathrm{Aut}_{\mathbb{F}_p}(V)$ is primitive of degree r and the action of C on $V \setminus \{1\}$ is simple and transitive.*

(2) *Conversely, to each primitive polynomial $f \in \mathbb{F}_p[X]$ of degree r, one may associate a faithful representation of C in* $\mathrm{Aut}_{\mathbb{F}_p}(V)$.

Remarks. (1) There is a one-to-one correspondence between the isomorphic irreducible representations ρ of C in V and the simple modules over $\mathbb{F}_p[C]$; these modules correspond to the irreducible divisors f of $X^{p^r-1} - 1$. In this bijection, a faithful representation corresponds to a primitive polynomial f.

(2) The tables of primitive polynomials f (see for instance [Ro, pp. 459–463] and [LN, Chapter 10, Tables E and F, pp. 564–566]), or Remark (2) following Definition 2.2, allow us to construct groups Γ which are defined by a faithful representation ρ; it suffices to use the companion matrix associated to f. Thus, it is easy to check that if $r = 1$ and $p = 3$, we may take (in fact we have to take) $f = 1 + X$ and Γ is isomorphic to the symmetric group S_3.

In all that follows in the present paper, we suppose that ρ is faithful. We denote by f the minimal polynomial of $\rho(\sigma)$ and by g the element of $\mathbb{F}_p[X]$ satisfying

$$fg = X^{p^r-1} - 1.$$

Recall that if $P \in K[X]$ has degree n, where K is any field, then the polynomial $\hat{P} = X^n P(X^{-1})$ is called the reciprocal polynomial of P. It is easily seen that if P is irreducible and $P(0) \neq 0$, then $\hat{P}$ is also irreducible.

Using a method analogous to that in the proof of [BGS, Proposition 2.4, p. 11], we obtain:

Proposition 2.4. *With the previous notation, the following assertions are equivalent*:

(i) *The extension N/k is Galois and* $\mathrm{Gal}(N/k) \simeq \Gamma = V \rtimes_\rho C$.
(ii) *There exists $m \in E^\times/E^{\times p}$ satisfying $\hat{g}(\sigma)m \neq 1$ and $W = \mathbb{F}_p[C]\hat{g}(\sigma)m$.*

Let $\bar{s}$ be the natural surjective morphism from $\mathbb{Z}[C]$ onto $\mathbb{F}_p[C]$.

From now on and until the end of the present paper, we will use the following abuse of notation: *we will also denote $\hat{g}(\sigma)$ the inverse image, by $\bar{s}$, of $\hat{g}(\sigma) \in \mathbb{F}_p[C]$, which has its coefficients in $\{0, 1, \ldots, p-1\}$; we will say that we consider $\hat{g}(\sigma)$ as an element of $\mathbb{N}[C]$, where $\mathbb{N} = \{0, 1, 2, \ldots\}$ is the set of natural numbers.*

An immediate consequence of the previous proposition is the following result, which is a criterion for a cyclic extension of degree $p^r - 1$ to be embeddable in an extension whose Galois group is isomorphic to Γ. This result generalizes Proposition 2.5 of [BGS] and will be useful in the proofs of the main results.

Proposition 2.5. *Let k be a number field, E/k a cyclic extension of degree $p^r - 1$ containing ξ_p, and L/E a cyclic extension of degree p. Then the following assertions are equivalent*:

(i) *The Galois closure of L/k is an extension N/k with Galois group isomorphic to Γ.*
(ii) *There exists $m \in E$ such that $L = E(\sqrt[p]{\hat{g}(\sigma)m})$, where we consider $\hat{g}(\sigma)$ as an element of $\mathbb{N}[C]$.*

Furthermore, if (ii) *is satisfied, we may choose N equal to the compositum of the extensions $E(\sqrt[p]{\sigma^i \hat{g}(\sigma)m})$, $0 \leqslant i \leqslant p^r - 2$.*

Below, we will give some definitions and results which will be useful in the subsequent sections.

Let $\alpha(\sigma) = \sum_{i=0}^{p^r-2} a_i \sigma^i$ be an element of the group ring $\mathbb{Z}[C]$, where $a_i \in \mathbb{Z}$.

We define the integral weight of $\alpha(\sigma)$, that will be denoted $w_{\mathrm{in}}(\alpha(\sigma))$, by $w_{\mathrm{in}}(\alpha(\sigma)) = \sum_{i=0}^{p^r-2} a_i$; in other words, it is the image of $\alpha(\sigma)$ by the augmentation morphism $\mathbb{Z}[C] \to \mathbb{Z}$.

We define the modular weight of $\alpha(\sigma)$, that we denote $w_{\mathrm{m}}(\alpha(\sigma))$, to be the number of coefficients a_i which are relatively prime to p.

Let k be a number field and I a (nonzero) fractional ideal of O_k. We call integral weight of I the number $w_{\mathrm{in}}(I)$ defined as $\sum_{\mathfrak{p}} v_{\mathfrak{p}}(I)$, where $\mathfrak{p}$ runs through the set of prime ideals of O_k and $v_{\mathfrak{p}}$ is the corresponding $\mathfrak{p}$-adic valuation. Immediately, we have $w_{\mathrm{in}}(IJ) = w_{\mathrm{in}}(I) + w_{\mathrm{in}}(J)$ for every fractional ideal J.

Clearly, the fractional ideal I can be written uniquely in the form:

$$I = J_0^p \prod_{i=1}^{p-1} J_i^i,$$

where J_0 is a fractional ideal of O_k, and the J_i, $1 \leqslant i \leqslant p-1$, are pairwise relatively prime square free integral ideals of O_k. The ideal J_0 will be called the p-part of I, and the ideal $\prod_{i=1}^{p-1} J_i$, which will be denoted by $\mathcal{F}(I)$, the conductor of I (for this terminology see Remark (3) following Proposition 3.2).

Remark. The p-part (respectively conductor) of a certain fractional ideal I is useful to calculate the realizable Galois module class (respectively Steinitz class) (see Section 4 (respectively Section 3)).

We recall the (simplest) definition of a cyclic code (see for instance [Ro, §7.4, p. 320]): it is an ideal of $\mathbb{F}_q[X]/(X^n - 1)$, where $\mathbb{F}_q$ is a finite field with q elements and n a nonzero natural integer; its elements are called codewords. In the terminology of coding theory (see for instance [Ro, p. 146]), the weight of a codeword of a cyclic code is the number of its nonzero components in the canonical basis $(\overline{1}, \overline{X}, \ldots, \overline{X}^{n-1})$.

In our situation, since $\mathbb{F}_p[C] \simeq \mathbb{F}_p[X]/(X^{p^r-1} - 1)$ (the isomorphism is given by $\sigma \mapsto \overline{X}$), one defines a cyclic code of $\mathbb{F}_p[C]$ as an ideal of $\mathbb{F}_p[C]$. Let $\overline{\alpha(\sigma)}$ be the image of an element $\alpha(\sigma) \in \mathbb{Z}[C]$ in $\mathbb{F}_p[C]$ by the natural surjective morphism $\bar{s}: \mathbb{Z}[C] \to \mathbb{F}_p[C]$. Then, $w_{\mathrm{m}}(\alpha(\sigma))$ is in fact the weight of $\overline{\alpha(\sigma)}$ as an element of any cyclic code.

We will say that $\overline{\alpha(\sigma)}$ is considered as an element of $\mathbb{N}[C]$ (as we did for $\hat{g}(\sigma)$), to mean that we identify $\overline{\alpha(\sigma)}$ with its inverse image (by $\bar{s}$) of which the coefficients belong to $\{0, 1, \ldots, p-1\}$.

Proposition 2.6. *The nonzero codewords of the cyclic code of $\mathbb{F}_p[C]$ generated by $\hat{g}(\sigma)$ have the same (modular) weight $p^{r-1}(p-1)$, and considered as elements of $\mathbb{N}[C]$, have the same integral weight $p^r(p-1)/2$.*

Proof. The morphism from $\mathbb{F}_p[C]$ to $\mathbb{F}_p[C]$, which to $h(\sigma)$ assigns $h(\sigma)\hat{g}(\sigma)$, gives $\mathbb{F}_p[C]/(\hat{f}(\sigma)) \simeq (\hat{g}(\sigma))$. Let i, $0 \leqslant i \leqslant p^r - 2$. We have $\sigma^i \equiv 1 \bmod \hat{f}(\sigma)$ if and only if $\hat{f}$ divides $X^i - 1$ (since $\mathbb{F}_p[C]/(\hat{f}(\sigma)) \simeq \mathbb{F}_p[X]/(\hat{f})$), which is equivalent to $i = 0$, because the order of the roots of $\hat{f}$ is $p^r - 1$, since they are the inverses of those of f. One deduces that the σ^i, $0 \leqslant i \leqslant p^r - 2$, are pairwise distinct modulo $\hat{f}(\sigma)$. As $\mathbb{F}_p[C]/(\hat{f}(\sigma))$ is an $\mathbb{F}_p$-vector space of dimension r, it is then equal to $\{\overline{0}, \overline{1}, \overline{\sigma}, \ldots, \overline{\sigma^{p^r-2}}\}$. It follows that $(\hat{g}(\sigma)) = \{0, \sigma^i \hat{g}(\sigma),\ 0 \leqslant i \leqslant p^r - 2\}$. We observe that $(\hat{g}(\sigma))$ consists simply of 0 and all the cyclic shifts of $\hat{g}(\sigma)$. It is hence clear that the codewords $\sigma^i \hat{g}(\sigma)$, $0 \leqslant i \leqslant p^r - 2$, have the same modular weight $w_{\mathrm{m}}(\hat{g}(\sigma))$ and, considered as elements of $\mathbb{N}[C]$, have the same integral weight $w_{\mathrm{in}}(\hat{g}(\sigma)) = \hat{g}(1)$.

By the previous observation, $w_{\mathrm{m}}(\hat{g}(\sigma))$ is equal to the cardinal of the set $\{x \in (\hat{g}(\sigma)) \mid \text{the 1st component of } x \text{ in the basis } C \text{ is nonzero}\}$. But this last set is the complement of a hyperplane of $(\hat{g}(\sigma))$. Consequently, $w_{\mathrm{m}}(\hat{g}(\sigma)) = p^r - p^{r-1} = p^{r-1}(p-1)$.

Now, let us calculate $w_{\mathrm{in}}(\hat{g}(\sigma))$. In the following discussion, we consider the codewords of $(\hat{g}(\sigma))$ as elements of $\mathbb{N}[C]$. We write $\hat{g}(\sigma) = \sum_{i=0}^{p^r-2} a_i \sigma^i$. Let $I_j = \{a_i \mid a_i = j\}$, where $1 \leqslant j \leqslant p-1$; I_1 is not empty: since g being monic, we have $a_0 = 1$. The cardinal of I_j

$(\mathrm{card}(I_j))$ is equal to that of I_1; indeed, we see this by observing that the number of the coefficients of the codeword $j\hat{g}(\sigma)$ which are equal to j is both $\mathrm{card}(I_1)$ and $\mathrm{card}(I_j)$. One deduces that $w_{\mathrm{in}}(\hat{g}(\sigma)) = \mathrm{card}(I_1)(1+2+\cdots+p-1) = \mathrm{card}(I_1)(p(p-1)/2)$. But $w_{\mathrm{m}}(\hat{g}(\sigma)) = \sum_{j=1}^{p-1} \mathrm{card}(I_j) = (p-1)\,\mathrm{card}(I_1)$. It follows that $w_{\mathrm{in}}(\hat{g}(\sigma)) = p^r(p-1)/2$. □

Remark. Proposition 2.6 is true even for $p = 2$ (in this case, $(\hat{g}(\sigma))$ is the dual of the binary Hamming code). It generalizes the well-known Lemma 3.6 of [BGS].

3. Steinitz classes

The purpose of this section is to prove Theorem 1.3. We recall that $\Gamma = V \rtimes_\rho C$, where V is an $\mathbb{F}_p$-vector space of dimension $r \geqslant 1$, p is an odd prime number, $C = \langle\sigma\rangle$ is a cyclic group of order $p^r - 1$, and ρ is a faithful representation of C in V. Recall also that f is the minimal polynomial of $\rho(\sigma)$ and g is the element of $\mathbb{F}_p[X]$ satisfying $fg = X^{p^r-1} - 1$.

We begin by fixing some notation and recalling well-known results which will be useful for the proof of Theorem 1.3.

Let k be a number field. If I is a fractional ideal of k, we denote by $\mathrm{cl}(I)$ its class in $\mathrm{Cl}(k)$. Let $\mathcal{C}$ be a cycle of k and $x \in k^\times$; the notation $x \equiv 1 \bmod^* \mathcal{C}$ will denote the usual relation of congruence mod* in class field theory (see [N]). If K/k is a finite extension of number fields, $[K : k]$ denotes its degree, $\Delta(K/k)$ its discriminant and $N_{K/k}$ (respectively $\mathrm{Tr}_{K/k}$) its norm map (respectively trace map). We recall that $\mathrm{cl}_k(O_K)$ is the Steinitz class of K/k. The following proposition is Proposition 3.1 of [BGS].

Proposition 3.1. *Let $k \subset K \subset M$ be a tower of number fields. Then*:

(i) $\mathrm{cl}_k(O_K) = \mathrm{cl}((\Delta(K/k)/d)^{1/2})$, *where d is the discriminant of a basis of the k-vector space K. Moreover, if K/k is Galois with odd degree, then* $\mathrm{cl}_k(O_K) = \mathrm{cl}((\Delta(K/k))^{1/2})$.
(ii) $\mathrm{cl}_k(O_M) = \mathrm{cl}_k(O_K)^{[M:K]} N_{K/k}(\mathrm{cl}_K(O_M))$.

Proof. The assertion (i) is a theorem of Artin (see [A]). The result (ii), which may be read as the transitivity of the Steinitz class in a tower of number fields, is Theorem 4.1 of [F1]. □

Let K be a number field containing ξ_p. Let M/K be a cyclic (Kummer) extension of degree p. Let $m \in K$ be such that $M = K(\sqrt[p]{m})$. We have seen at the end of Section 2 that the fractional ideal mO_K can be written uniquely in the form:

$$mO_K = \big(I(m)\big)^p \prod_{i=1}^{p-1} J_i^i, \tag{3.1}$$

where $I(m)$ is the p-part of mO_K, the J_i, $1 \leqslant i \leqslant p-1$, are pairwise relatively prime square free integral ideals of O_K, and $\mathcal{F}(mO_K) = \prod_{i=1}^{p-1} J_i$ is the conductor of mO_K.

The following proposition results immediately from Kummer theory (see [H, §39], or [Co2, §10.2]) and the above theorem of Artin.

Proposition 3.2. *With the preceding notation, we have*:

(i) $\Delta(M/K) = (\mathcal{F}(mO_K)J)^{p-1}$, *where J is an integral ideal of O_K whose prime divisors divide pO_K. The extension M/K is tame if and only if there exists $b \in O_K$ such that*

$b^p m \equiv 1 \bmod^* (1-\xi_p)^p O_K$; *this condition is equivalent to* $J = O_K$ *and* $\mathcal{F}(mO_K)$ *is relatively prime to* pO_K.

(ii) $\mathrm{cl}_K(O_M) = \mathrm{cl}((\mathcal{F}(mO_K)J)^{p-1/2})$.

Remarks. (1) In the case of tame ramification, the conductor of mO_K determines the Steinitz class of M/K.

(2) We point out a difference between [BGS] and the present paper: let M'/K' be a quadratic extension, and let $m \in K'$ be such that $M' = K'(\sqrt{m})$, then we can write (3.1) with $p = 2$; when M'/K' is tame, in [BGS, Remark after Proposition 3.2] the 2-part (not the conductor J_1) of mO_K determines the Steinitz class of M'/K' (here we extend the definition of p-part and conductor to $p = 2$).

(3) Let χ be a nontrivial character of $\mathrm{Gal}(M/K)$ and $\mathcal{F}(\chi)$ its Artin conductor. By the formula of Artin and Hasse (the Führerdiskriminantenproduktformel) (see [Se2, Chapter VI]), $\Delta(M/K) = (\mathcal{F}(\chi))^{p-1}$. If M/K is tame, then $\mathcal{F}(\chi) = \mathcal{F}(mO_K)$ by the previous proposition; this justifies the terminology of conductor of an ideal which has been introduced in Section 2.

In this section, N/k is a Galois extension whose Galois group is isomorphic to Γ. If π is an isomorphism from $\mathrm{Gal}(N/k)$ to Γ and if $\gamma \in \Gamma$, one identifies $\pi^{-1}(\gamma)$ with γ. Let E/k be the subextension of N fixed by V. Then E/k is cyclic of degree $p^r - 1$ and $\mathrm{Gal}(E/k) \simeq C$. The extension N/E contains $u = (p^r-1)/(p-1)$ cyclic subextensions of E of degree p; if L/E is one of these, then the others have the form $\sigma^i(L)$, $1 \leqslant i \leqslant p^r - 2$ (i is not unique; but if $u \neq 1$, i.e. $r \neq 1$, we can take $1 \leqslant i \leqslant u-1$ so that i is unique).

Proposition 3.3. *With the above notation we have*:

$$\mathrm{cl}_k(O_N) = \big(\mathrm{cl}_k(O_E)\big)^{p^r} \big(N_{E/k}\big(\mathrm{cl}_E(O_L)\big)\big)^u.$$

The following lemma will be useful for the proof of the previous proposition.

Lemma 3.4. *Let* K *be a number field,* M/K *a Galois extension with Galois group* V*, and let* K_i/K*,* $1 \leqslant i \leqslant u$*, be the cyclic subextensions of* M/K *of degree* p*. Then*

$$\mathrm{cl}_K(O_M) = \prod_{i=1}^{u} \mathrm{cl}_K(O_{K_i}).$$

Proof of Lemma 3.4 and Proposition 3.3. The proof of Lemma 3.4 is essentially the same as that given in [BGS, Lemma 3.4, p. 14]; the calculation of d and the d_i in that proof can be omitted since the degrees of M/K and K_i/K are odd (see Proposition 3.1(i)). To get Proposition 3.3, it suffices to proceed as in the proof of [BGS, Proposition 3.3, p. 14]. □

The group I_E of fractional ideals of E is, in a natural way, a $\mathbb{Z}[C]$-module. We choose exponential notation for the action of $\mathbb{Z}[C]$ on I_E: if $I \in I_E$ and $\alpha(\sigma) = \sum_{i=0}^{p^r-2} a_i \sigma^i \in \mathbb{Z}[C]$, then

$$I^{\alpha(\sigma)} = \prod_{i=0}^{p^r-2} \sigma^i(I)^{a_i}.$$

It is easily seen that $w_{\mathrm{in}}(I^{\alpha(\sigma)}) = w_{\mathrm{in}}(\alpha(\sigma)) w_{\mathrm{in}}(I)$.

Proposition 3.5. *Let $\mathfrak{P}$ be a prime ideal of O_E and $e(\sigma) \in \mathbb{Z}[C]$.*

(1) *If $\mathfrak{P} \cap O_k$ is not totally split in E/k or $e(\sigma)\hat{g}(\sigma) = 0$ in $\mathbb{F}_p[C]$, then $\mathcal{F}(\mathfrak{P}^{e(\sigma)\hat{g}(\sigma)}) = O_E$.*
(2) *Otherwise, $N_{E/k}(\mathcal{F}(\mathfrak{P}^{e(\sigma)\hat{g}(\sigma)})) = N_{E/k}(\mathfrak{P})^{p^{r-1}(p-1)}$.*

Proof. (1) The case where the element $e(\sigma)\hat{g}(\sigma)$ is 0 in $\mathbb{F}_p[C]$ is trivial; in what follows, this element is assumed to be nonzero. Suppose that $\mathfrak{P} \cap O_k$ is not totally split in E/k. Arguing as in part (2) of the proof of [BGS, Proposition 3.5, p. 15], we obtain $\mathfrak{P}^{\hat{g}(\sigma)}$ is a pth power of an ideal of O_E, thus so is $\mathfrak{P}^{e(\sigma)\hat{g}(\sigma)}$, hence we have the assertion (1).

(2) Suppose that $\mathfrak{P} \cap O_k$ is totally split in E/k. We let $\alpha(\sigma) = e(\sigma)\hat{g}(\sigma)$. Clearly one may write $\alpha(\sigma) = pq(\sigma) + r(\sigma)$, where the coefficients a_i in the basis C of $r(\sigma)$ belong to $\{0, 1, \ldots, p-1\}$. As $\mathfrak{P}^{\alpha(\sigma)} = (\mathfrak{P}^{q(\sigma)})^p \mathfrak{P}^{r(\sigma)}$ and $\mathfrak{P} \cap O_k$ is totally split in E/k, we have $\mathcal{F}(\mathfrak{P}^{e(\sigma)\hat{g}(\sigma)}) = \prod_{i,\, a_i \neq 0} \sigma^i(\mathfrak{P})$. We deduce that $N_{E/k}(\mathcal{F}(\mathfrak{P}^{e(\sigma)\hat{g}(\sigma)})) = N_{E/k}(\mathfrak{P})^{w_{\mathrm{m}}(r(\sigma))}$. It is clear that $w_{\mathrm{m}}(r(\sigma)) = w_{\mathrm{m}}(e(\sigma)\hat{g}(\sigma))$. But $w_{\mathrm{m}}(e(\sigma)\hat{g}(\sigma)) = w_{\mathrm{m}}(\overline{e(\sigma)\hat{g}(\sigma)})$, where $\overline{e(\sigma)\hat{g}(\sigma)}$ is the image of $e(\sigma)\hat{g}(\sigma)$ in the cyclic code $(\hat{g}(\sigma))$ of $\mathbb{F}_p[C]$ (see the paragraph before Proposition 2.6 in Section 2). We then conclude that (2) holds thanks to Proposition 2.6. □

Proof of Theorem 1.3(i). Let us prove the first inclusion

$$R_t(E/k, \Sigma) \subset \mathrm{cl}_k(O_E)^{p^r} \big(N_{E/k}\big(\mathrm{Cl}(E)\big)\big)^{p^{r-1}(p^r-1)(p-1)/2}. \tag{3.2}$$

Let N/k be a tame Galois extension with Galois group isomorphic to Γ. Let $L = E(\sqrt[p]{\hat{g}(\sigma)m})/E$ be a subextension of N/E of degree p (see Proposition 2.5). As in (3.1), we have the (unique) decomposition

$$\hat{g}(\sigma)m\,O_E = \big[I\big(\hat{g}(\sigma)m\big)\big]^p \prod_{i=1}^{p-1} J_i^i,$$

where $I(\hat{g}(\sigma)m)$ is the p-part of $\hat{g}(\sigma)m\,O_E$, the J_i, $1 \leqslant i \leqslant p-1$, are pairwise relatively prime square free integral ideals of O_E, and $\mathcal{F}(\hat{g}(\sigma)m\,O_E) = \prod_{i=1}^{p-1} J_i$ is the conductor of $\hat{g}(\sigma)m\,O_E$. Since L/E is tame, by virtue of Proposition 3.2 we have

$$\mathrm{cl}_E(O_L) = \mathrm{cl}\big(\mathcal{F}\big(\hat{g}(\sigma)m\,O_E\big)^{(p-1)/2}\big).$$

We may write

$$m\,O_E = \prod_{i=1}^{s} \mathfrak{P}_i^{e_i(\sigma)},$$

where $s \geqslant 1$, $e_i(\sigma) \in \mathbb{Z}[C]$, and the $\mathfrak{P}_i$ are prime ideals of O_E which are above distinct prime ideals of O_k; consequently, the ideals $\mathfrak{P}_i^{e_i(\sigma)}$ are pairwise relatively prime. (We point out that $e_i(\sigma)$ are not unique, except in the case where all the $\mathfrak{P}_i \cap O_k$ are totally split in E/k.) We have

$$\hat{g}(\sigma)m\,O_E = \prod_{i=1}^{s} \mathfrak{P}_i^{e_i(\sigma)\hat{g}(\sigma)}.$$

Since the ideals $\mathfrak{P}_i^{e_i(\sigma)\hat{g}(\sigma)}$ are pairwise relatively prime, it is immediate that

$$\mathcal{F}\big(\hat{g}(\sigma)m\,O_E\big) = \prod_{i=1}^{s} \mathcal{F}\big(\mathfrak{P}_i^{e_i(\sigma)\hat{g}(\sigma)}\big).$$

By Proposition 3.5, we have

$$N_{E/k}\big(\mathcal{F}\big(\hat{g}(\sigma)m\,O_E\big)\big) = N_{E/k}(I')^{p^{r-1}(p-1)},$$

where I' is an integral ideal of O_E. We deduce the existence of $c \in \mathrm{Cl}(E)$ satisfying

$$N_{E/k}\big(\mathrm{cl}_E(O_L)\big) = N_{E/k}(c)^{p^{r-1}(p-1)^2/2}. \tag{3.3}$$

Proposition 3.3 and (3.3) give

$$\mathrm{cl}_k(O_N) = \big(\mathrm{cl}_k(O_E)\big)^{p^r} \big(N_{E/k}(c)\big)^{p^{r-1}(p^r-1)(p-1)/2},$$

which implies (3.2).

Let us now show the second inclusion:

$$\mathrm{cl}_k(O_E)^{p^r} \big(N_{E/k}\big(\mathrm{Cl}(E)\big)\big)^{p^{r-1}(p^r-1)(p-1)/2} \subset R_t(E/k, \Sigma). \tag{3.4}$$

Let $c \in \mathrm{Cl}(E)$. Let $t \geqslant 5$ be a natural odd integer such that $c^t = c$; for instance $t = 6h+1$, where h is the class number of E or the order of c. Let a_i, $1 \leqslant i \leqslant t$, be natural integers relatively prime to p and such that $\sum_{i=1}^{t} a_i = pt$; for instance: $a_i = p-1$, for $1 \leqslant i \leqslant (t+1)/2$, $a_i = p+1$, for $(t+3)/2 \leqslant i \leqslant t-1$, and $a_t = p+2$. Denote by $\mathrm{Cl}(E, (1-\xi_p)^p O_E)$ the ray class group of E modulo $(1-\xi_p)^p O_E$. By the canonical surjection from $\mathrm{Cl}(E, (1-\xi_p)^p O_E)$ onto $\mathrm{Cl}(E)$ and Tchebotarev density theorem (see [N, Chapter V, Theorem 6.4, p. 132]), there exist t prime ideals $\mathfrak{P}_i$ of O_E, above distinct prime ideals of O_k, totally split in E/k, relatively prime to $(1-\xi_p)^p O_E$ and such that $c = \mathrm{cl}(\mathfrak{P}_i)$ in $\mathrm{Cl}(E, (1-\xi_p)^p O_E)$. Similarly, let $\mathfrak{Q}$ be a prime ideal of O_E (not necessarily totally split in E/k) such that $c^{-1} = \mathrm{cl}(\mathfrak{Q})$ in $\mathrm{Cl}(E, (1-\xi_p)^p O_E)$. Then

$$\mathrm{cl}\left(\prod_{i=1}^{t} \mathfrak{P}_i^{a_i}\right) \mathrm{cl}\big(\mathfrak{Q}^{pt}\big) = 1 \quad \text{in } \mathrm{Cl}\big(E, (1-\xi_p)^p O_E\big).$$

Therefore, there exists $m \in E^\times$ satisfying

$$m\,O_E = \big(\mathfrak{Q}^t\big)^p \prod_{i=1}^{t} \mathfrak{P}_i^{a_i} \quad \text{and} \quad m \equiv 1 \mod^* (1-\xi_p)^p O_E.$$

Now we consider $\hat{g}(\sigma)$ as an element of $\mathbb{N}[C]$. We have the equality

$$\hat{g}(\sigma)m\,O_E = \big(\mathfrak{Q}^{t\hat{g}(\sigma)}\big)^p \prod_{i=1}^{t} \mathfrak{P}_i^{a_i\hat{g}(\sigma)}.$$

Clearly, $\hat{g}(\sigma)m$ is not a pth power of an element in E (for instance $v_{\mathfrak{P}_1}(\hat{g}(\sigma)m) \equiv a_1 \bmod p$; recall that $\hat{g}(0) = 1$, since g is monic). We consider the extension $L = E(\sqrt[p]{\hat{g}(\sigma)m})/E$ of degree p. According to Proposition 2.5, the Galois closure of L/k is an extension N/k with Galois group isomorphic to Γ, and we can take the compositum $N = E(\sqrt{\sigma^i \hat{g}(\sigma)m},\ 0 \leqslant i \leqslant p^r - 2)$. From $m \equiv 1 \bmod^* (1-\xi_p)^p O_E$ we deduce that for all i, $0 \leqslant i \leqslant p^r - 2$, $\sigma^i(m) \equiv 1 \bmod^* (1-\xi_p)^p O_E$. Thus $\hat{g}(\sigma)m \equiv 1 \bmod^* (1-\xi_p)^p O_E$ and $\sigma^i \hat{g}(\sigma)m \equiv 1 \bmod^* (1-\xi_p)^p O_E$. By Proposition 3.2(i), the extensions $E(\sqrt{\sigma^i \hat{g}(\sigma)m})/E$ are tame and then N/E is also tame. Suppose that E/k is tame. Then N/k is also tame.

Let us now calculate $N_{E/k}(\mathrm{cl}_E(O_L))$. As the ideals $\mathfrak{P}_i^{a_i \hat{g}(\sigma)}$ are pairwise relatively prime, we have

$$\mathcal{F}\big(\hat{g}(\sigma)m O_E\big) = \prod_{i=1}^{t} \mathcal{F}\big(\mathfrak{P}_i^{a_i \hat{g}(\sigma)}\big).$$

Since the ideals $\mathfrak{P}_i$ are totally split in E/k and $a_i \hat{g}(\sigma) \neq 0$ in $\mathbb{F}_p[C]$, Proposition 3.5 gives us

$$N_{E/k}\big(\mathcal{F}\big(\hat{g}(\sigma)m O_E\big)\big) = \prod_{i=1}^{t} N_{E/k}(\mathfrak{P}_i)^{p^{r-1}(p-1)}.$$

Because $c = \mathrm{cl}(\mathfrak{P}_i)$ and $c^t = c$, we deduce:

$$N_{E/k}\big(\mathrm{cl}\big(\mathcal{F}\big(\hat{g}(\sigma)m O_E\big)\big)\big) = N_{E/k}(c)^{p^{r-1}(p-1)}.$$

Using Proposition 3.2(ii), it follows that

$$N_{E/k}\big(\mathrm{cl}_E(O_L)\big) = N_{E/k}(c)^{p^{r-1}(p-1)^2/2}.$$

Applying Proposition 3.3, we obtain

$$\mathrm{cl}_k(O_N) = \big(\mathrm{cl}_k(O_E)\big)^{p^r} \big(N_{E/k}(c)\big)^{p^{r-1}(p^r-1)(p-1)/2}.$$

Hence we have (3.4), which completes the proof of the assertion (i) of Theorem 1.3. □

Remark. The difference between the previous proof and the proof of Theorem 1.4(i) in [BGS, §3, p. 16] comes from Remark 2 following Proposition 3.2: here we need to calculate the conductor (not the p-part) of $\hat{g}(\sigma)m O_E$.

Proof of Theorem 1.3(ii). Analogous to the proof of Theorem 1.4(ii) in [BGS, §3, p. 18]. □

Proof of Corollary 1.4. (i) According to the definition of Steinitz class, O_E is a free O_k-module if and only if $\mathrm{cl}_k(O_E) = 1$, whence we have (i) by Theorem 1.3(i).

(ii) Since $\xi_{p^r-1} \in k$, C is cyclic and $p^r - 1$ is even, we have $R_t(k, C) = \mathrm{Cl}(k)$ by Theorem 2 of [M1]. It follows from Theorem 1.3(ii) that

$$R_t(k, \Gamma) = \big(\mathrm{Cl}(k)^{p^{r-1}}\big)^p \big(\mathrm{Cl}(k)^{p^{r-1}}\big)^{(p^r-1)(p-1)/2}.$$

To complete the proof, it suffices to observe that the integers p and $(p^r-1)(p-1)/2$ are relatively prime. The particular case $\Gamma = S_3$ corresponds to $p=3$ and $r=1$. □

4. Realizable Galois module classes

The purpose of this section is to prove Theorem 1.1. Recall that the situation is the following: p is an odd prime number, k is a number field containing a primitive pth root of unity ξ_p, $\Gamma = V \rtimes_\rho C$, where V is an $\mathbb{F}_p$-vector space of dimension $r \geqslant 1$, $C = \langle\sigma\rangle$ is a cyclic group of order p^r-1, and ρ is a faithful representation of C in V.

To determine the conjugacy classes over k of the absolutely irreducible characters of Γ, we will proceed as in [BGS, §4].

The commutator subgroup $[\Gamma,\Gamma]$ of Γ may be identified with $(\sigma-1)V$. But $(\sigma-1)V = V$, because V is a simple $\mathbb{F}_p[C]$-module. Similarly, $(\sigma^i-1)V = V$ for all i, $1 \leqslant i \leqslant p^r-2$. One deduces that for all i in that interval, the element $\sigma^i v$ is conjugate to σ^i, for all $v \in V$. On the other hand, the elements σ^i and σ^j are not conjugate if $i \neq j$, because their images in the abelian group $\Gamma/V = C$ are distinct. The $v \neq 1$ are conjugate since the action of C on $V\setminus\{1\}$ is transitive. We conclude that the group Γ has exactly the following p^r conjugacy classes: the class $\{1\}$, the class $V\setminus\{1\}$, and the classes $\{\sigma^i v,\ v \in V\}$, with $1 \leqslant i \leqslant p^r-2$. Therefore (see [Se1]), Γ has p^r absolutely irreducible characters. There are exactly p^r-1 (linear) characters of degree 1 among them. They come from the characters of the group $\Gamma/[\Gamma,\Gamma]$ (which can be identified with C), and will be denoted by φ_i, $0 \leqslant i \leqslant p^r-2$, with φ_i defined by

$$\varphi_i(\sigma) = \xi_{p^r-1}^i, \quad \varphi_i(v) = 1 \quad \text{for all } v \in V,$$

where ξ_{p^r-1} is a primitive (p^r-1)th root of unity.

There remains only one irreducible character which will be denoted by χ. By the formula $\sum_{i=0}^{p^r-2} \varphi_i(1)^2 + \chi(1)^2 = |\Gamma| = p^r(p^r-1)$ (see [Se1, §2.4, Corollary 2, p. 18]), the degree of χ is p^r-1. Let ψ be a nontrivial irreducible complex character of V. Let us show that χ is induced by ψ, i.e., $\chi = \operatorname{Ind}_V^\Gamma \psi$.

Since for all i, $0 \leqslant i \leqslant p^r-2$, φ_i is trivial on V and $\sum_{v\in V}\psi(v) = 0$, by the Frobenius reciprocity formula (see [Se1, §7.2, Theorem 13, p. 56, and Remark 2 following it]), we have that $\operatorname{Ind}_V^\Gamma \psi$ is orthogonal to all the φ_i. As the degree of $\operatorname{Ind}_V^\Gamma \psi$ is equal to $|\Gamma/V| = p^r-1$, $\chi = \operatorname{Ind}_V^\Gamma \psi$.

Remark. By the formula which gives the values of $\operatorname{Ind}_V^\Gamma \psi$ (see [Se1, §3.3, Theorem 12, p. 30]), we check easily that for all i, $1 \leqslant i \leqslant p^r-2$, $\operatorname{Ind}_V^\Gamma \psi(\sigma^i) = 0$, and for all $v \in V\setminus\{1\}$, $\operatorname{Ind}_V^\Gamma \psi(v) = -1$. We deduce that χ has its values in $\{0,-1,p^r-1\}$.

Let $n+1$ be the number of conjugacy classes over k of the characters φ_i, and $\{\psi_i, 0 \leqslant i \leqslant n\}$ a set of their representatives, with ψ_0 the trivial character. Then Γ has $n+2$ conjugacy classes of absolutely irreducible characters over k having the representatives ψ_i, $0 \leqslant i \leqslant n$, and $\psi_{n+1} = \chi$.

For all i, $1 \leqslant i \leqslant n$, the restriction of ψ_i to C defines a nontrivial character of C, because $\operatorname{Ker}(\psi_i) \supset V$; this will be denoted by χ_i. Let χ_0 be the trivial character of C. Clearly $\{\chi_i,\ 0 \leqslant i \leqslant n\}$ is a set of representatives of all conjugacy classes over k of absolutely irreducible characters of C (this is the notation of the introduction). Let $k(\psi_i)$ (respectively $k(\chi_i)$) be the extension of k obtained by adjoining to k the values of ψ_i (respectively χ_i). Then $k(\psi_i) = k(\chi_i)$ for all i, $0 \leqslant i \leqslant n$.

The Wedderburn decomposition of $k[\Gamma]$ as a product of simple algebras is (see [CR2, p. 330 and §74])

$$k[\Gamma] = \prod_{i=0}^{n+1} M_{n_i}(D_i),$$

where D_i is a skewfield with center $k(\psi_i)$ and $M_{n_i}(D_i)$ is the ring of $n_i \times n_i$ matrices with coefficients in D_i. We recall that the dimension of D_i over $k(\psi_i)$ is a square m_i^2, where m_i is the Schur index relative to k. Thus $\chi_i(1) = n_i m_i$.

It is obvious that $m_i = 1$ for $0 \leqslant i \leqslant n$. Also, $m_{n+1} = 1$ since χ is realizable over k: recall that χ is induced by ψ, and ψ is realizable over k because V has exponent p. One deduces immediately that

$$k[\Gamma] \simeq \prod_{i=0}^{n} k(\psi_i) \times M_{p^r-1}(k) = \prod_{i=0}^{n} k(\chi_i) \times M_{p^r-1}(k).$$

Let $\mathcal{M}$ be a maximal O_k-order in $k[\Gamma]$ containing $O_k[\Gamma]$. Suppose $p \neq 3$ or $r \neq 1$; since no simple component of $k[\Gamma]$ has dimension 4 over its center, $k[\Gamma]$ satisfies the Eichler condition (see [R, Definition 38.1, pp. 343–344; Remark (34.4), p. 294]). It is easy to check that $k[S_3]$ (the case $p = 3$ and $r = 1$) also satisfies the Eichler condition. Consequently, by a result of Swan (see [Sw] or [R, Theorem 35.14, p. 313]), and since $D_i = k(\psi_i)$ for all $0 \leqslant i \leqslant n+1$, we have

$$\mathrm{Cl}(\mathcal{M}) \simeq \prod_{i=0}^{n} \mathrm{Cl}\big(k(\psi_i)\big) \times \mathrm{Cl}(k) = \prod_{i=0}^{n} \mathrm{Cl}\big(k(\chi_i)\big) \times \mathrm{Cl}(k).$$

Whence

$$\mathrm{Cl}^\circ(\mathcal{M}) \simeq \prod_{i=1}^{n} \mathrm{Cl}\big(k(\chi_i)\big) \times \mathrm{Cl}(k) \simeq \mathrm{Cl}^\circ\big(\mathcal{M}(C)\big) \times \mathrm{Cl}(k). \tag{4.1}$$

Let K be any number field and Γ' a finite group such that $K[\Gamma']$ satisfies the Eichler condition. Let $\mathcal{M}'$ be an O_K-maximal order in $K[\Gamma']$ containing $O_K[\Gamma']$. Below, we will recall briefly Fröhlich's Hom-description of the locally free class group $\mathrm{Cl}(\mathcal{M}')$ (see [F2,F4] or [CR2, §52]), and Fröhlich–Lagrange resolvent (see [F4, pp. 28–29]).

We write $R_{\Gamma'}$ for the group of virtual characters of Γ'. Let $\overline{K}$ be an algebraic closure of K, $\Omega_K = \mathrm{Gal}(\overline{K}/K)$, $J(\overline{K})$ the group of ideles of $\overline{K}$, and $U(\overline{K})$ the subgroup of unit ideles of $J(\overline{K})$. Then

$$\mathrm{Cl}(\mathcal{M}') \simeq \frac{\mathrm{Hom}_{\Omega_K}(R_{\Gamma'}, J(\overline{K}))}{\mathrm{Hom}_{\Omega_K}(R_{\Gamma'}, \overline{K}^\times)\,\mathrm{Hom}_{\Omega_K}(R_{\Gamma'}, U(\overline{K}))}.$$

Let M/K be a Galois extension whose Galois group is isomorphic to Γ'. If π is an isomorphism from $\mathrm{Gal}(M/K)$ to Γ', then any character χ' of Γ' induces a character $\chi' \circ \pi$ of $\mathrm{Gal}(M/K)$ which we will also denote by χ'. If $\gamma \in \Gamma'$, we shall also denote $\pi^{-1}(\gamma) \in \mathrm{Gal}(M/K)$ simply by γ. Let B be a commutative K-algebra. Then $M \otimes_K B$ is a free $B[\Gamma']$-module of rank 1; let $a \in M \otimes_k B$ be a basis of this module. Let $T : \Gamma' \to GL_{n'}(\overline{K})$ be a linear

representation of Γ' with character χ'. The Fröhlich–Lagrange resolvent $\langle a, \chi'\rangle_{M/K}$ (or simply $\langle a, \chi'\rangle$ if no confusion arises) with respect to M/K is the element of $\overline{K} \otimes_K B$ defined by

$$\langle a, \chi'\rangle_{M/K} = \mathrm{Det}\Big(\sum_{\gamma\in\Gamma'} \gamma(a) T\big(\gamma^{-1}\big)\Big),$$

where Det is the determinant.

Now we fix some notation. For each prime $\mathfrak{p}$ of O_K, let $K_\mathfrak{p}$ (respectively $O_{K,\mathfrak{p}}$) be the completion of K (respectively O_K) at $\mathfrak{p}$. Let $M_\mathfrak{p} = M \otimes_K K_\mathfrak{p}$ and $O_{M,\mathfrak{p}} = O_M \otimes_{O_K} O_{K,\mathfrak{p}}$ be the semilocal completion of M and O_M at $\mathfrak{p}$, respectively.

Suppose that M/K is tame. One knows that O_M is a locally free $O_K[\Gamma']$-module of rank 1. For each prime ideal $\mathfrak{p}$ of O_K, let $\alpha_\mathfrak{p}$ be a basis of the $O_{K,\mathfrak{p}}[\Gamma]$-module $O_{M,\mathfrak{p}}$ (i.e., $\alpha_\mathfrak{p}$ generates a local normal integral basis). Let a be a basis of the $K[\Gamma']$-module M (i.e., a generates a normal basis of M/K). By a result of Fröhlich (see [F4]), a representative of the class of $\mathcal{M}' \otimes_{O_K[\Gamma']} O_M$, which will be denoted $[\mathcal{M}' \otimes_{O_K[\Gamma']} O_M]$, in $\mathrm{Cl}(\mathcal{M}')$ is the following map h:

$$h(\chi') = \left(\frac{\langle \alpha_\mathfrak{p}, \chi'\rangle}{\langle a, \chi'\rangle}\right)_\mathfrak{p}.$$

From now on, N/k is a tame Galois extension whose Galois group is isomorphic to Γ. We denote by E the subextension of N fixed by V. In what follows, we will determine an element h of $\mathrm{Hom}_{\Omega_k}(R_\Gamma, J(\bar{k}))$ which is a representative of $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ in $\mathrm{Cl}(\mathcal{M})$ by calculating its values at ψ_i, $0 \leqslant i \leqslant n$, and at χ.

Let a be a basis of the $k[\Gamma]$-module N. For every prime ideal $\mathfrak{p}$ of O_k, let $\alpha_\mathfrak{p}$ be a basis of the $O_{k,\mathfrak{p}}[\Gamma]$-module $O_{N,\mathfrak{p}}$.

Let i, $1 \leqslant i \leqslant n$. The following equalities follow immediately from the definition of Fröhlich–Lagrange resolvent (one may see [F3, Theorem 10, p. 162]):

$$\langle \alpha_\mathfrak{p}, \psi_i\rangle = \big\langle \mathrm{Tr}_{N_\mathfrak{p}/E_\mathfrak{p}}(\alpha_\mathfrak{p}), \chi_i\big\rangle_{E/k}, \tag{4.2}$$

$$\langle a, \psi_i\rangle = \big\langle \mathrm{Tr}_{N/E}(a), \chi_i\big\rangle_{E/k}. \tag{4.3}$$

We point out that $\mathrm{Tr}_{N_\mathfrak{p}/E_\mathfrak{p}}(\alpha_\mathfrak{p})$ and $\mathrm{Tr}_{N/E}(a)$ are, respectively, bases of the $O_{k,\mathfrak{p}}[C]$-module $O_{E,\mathfrak{p}}$ and the $k[C]$-module E.

Let b and $b_\mathfrak{p}$ be bases of the $E[V]$-module N and the $O_{E,\mathfrak{p}}[V]$-module $O_{N,\mathfrak{p}}$, respectively. As in [BGS, (4.4) and (4.5), p. 22], let $e(E/k) \in k$ be such that $e(E/k)^2$ is the discriminant of a basis of the k-vector space E, let $e(E_\mathfrak{p}/k_\mathfrak{p}) \in O_{k,\mathfrak{p}}$ be such that $e(E_\mathfrak{p}/k_\mathfrak{p})^2 O_{k,\mathfrak{p}}$ is the discriminant of $E_\mathfrak{p}/k_\mathfrak{p}$, and we let $\mathfrak{N}_{E/k}(\langle x, \psi\rangle_{N/E}) = \prod_{\gamma\in\mathrm{Gal}(E/k)} \gamma(\langle x, \gamma^{-1}\psi\rangle_{N/E})$. We have $\mathfrak{N}_{E/k} = N_{E/k}$ because $\xi_p \in k$.

Now using a method similar to that in the proof of [BGS, Proposition 4.1, pp. 22–23], we obtain the following proposition.

Proposition 4.1. *With the above hypotheses and notation, a representative of the class of* $\mathcal{M} \otimes_{O_k[\Gamma]} O_N$ *in* $\mathrm{Cl}(\mathcal{M})$ *is the element* h *of* $\mathrm{Hom}_{\Omega_k}(R_\Gamma, J(\bar{k}))$ *defined by*

$$h(\psi_0) = (1),$$

$$h(\psi_i) = \left(\frac{\langle \mathrm{Tr}_{N_\mathfrak{p}/E_\mathfrak{p}}(\alpha_\mathfrak{p}), \chi_i \rangle_{E/k}}{\langle \mathrm{Tr}_{N/E}(a), \chi_i \rangle_{E/k}} \right)_\mathfrak{p}, \quad \text{for all } i, 1 \leqslant i \leqslant n,$$

$$h(\chi) = \left(\frac{e(E_\mathfrak{p}/k_\mathfrak{p})}{e(E/k)} N_{E/k} \left(\frac{\langle b_\mathfrak{p}, \psi \rangle_{N/E}}{\langle b, \psi \rangle_{N/E}} \right) \right)_\mathfrak{p}.$$

We recall (with the notation of Section 1) that $\mathcal{M}(C)$ is the maximal O_k-order in $k[C]$, $\mathcal{R}(\mathcal{M}(C))$ is the set of those classes in $\mathrm{Cl}(\mathcal{M}(C))$ which are realizable by tame Galois extensions of k whose Galois group is isomorphic to C, and $\mathcal{R}(\mathcal{M}(C))$ is a subgroup of $\mathrm{Cl}^\circ(\mathcal{M}(C)) \simeq \prod_{i=1}^n \mathrm{Cl}(k(\chi_i))$. In the sequel, we will often identify $\mathrm{Cl}^\circ(\mathcal{M}(C))$ with $\prod_{i=1}^n \mathrm{Cl}(k(\chi_i))$ under the preceding isomorphism.

Proposition 4.2. *Let c_i, $0 \leqslant i \leqslant n+1$, be the components of $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N]$ in $\prod_{i=0}^n \mathrm{Cl}(k(\chi_i)) \times \mathrm{Cl}(k))$. Then*:

(i) *c_0 is the trivial class in $\mathrm{Cl}(k)$.*
(ii) *$(c_1, c_2, \ldots, c_n)$ is the class of $[\mathcal{M}(C) \otimes_{O_k[C]} O_E]$ in $\prod_{i=1}^n \mathrm{Cl}(k(\chi_i))$.*
(iii) *Let $L = E(\sqrt[p]{\hat{g}(\sigma)m})/E$ be a subextension of N/E of degree p. As in* (3.1)*, let the* (*unique*) *decomposition of $\hat{g}(\sigma)m\,O_E$ be*

$$\hat{g}(\sigma)m\,O_E = \left[I\left(\hat{g}(\sigma)m\right) \right]^p \prod_{i=1}^{p-1} J_i^i.$$

Then, $c_{n+1} = \mathrm{cl}_k(O_E) N_{E/k}(\mathrm{cl}((I(\hat{g}(\sigma)m))^{-1}))$ in $\mathrm{Cl}(k)$.

Remark. The main difference between the previous proposition and [BGS, Proposition 4.2, p. 23] is in the assertion (iii): here $\mathrm{cl}((I(\hat{g}(\sigma)m))^{-1})$ replaces the Steinitz class of L/E (which is the case in [BGS]). This fact will imply a difference between the proof of our Theorem 1.1 and the proof of Theorem 1.1 in [BGS, §4, p. 25].

We will need a lemma to prove the assertion (iii) of Proposition 4.2. To state this lemma, we begin by fixing some notation.

Let K be a number field containing ξ_p. Let M/K be a tame cyclic extension of degree p. Let ϕ be a nontrivial irreducible complex character of $\mathrm{Gal}(M/K)$ (equivalently: a morphism from $\mathrm{Gal}(M/K)$ to $\mathbb{C}^\times$ of order p). We denote by $\langle O_M, \phi \rangle$ the set consisting of the elements $\langle x, \phi \rangle_{M/K}$ (or simply $\langle x, \phi \rangle$), where x varies in O_M. Let c be a normal basis of M/K. Since for all $\gamma \in \mathrm{Gal}(M/K)$ and $x \in M$, $\gamma(\langle x, \phi \rangle) = \phi(\gamma)\langle x, \phi \rangle$ (which is easily checked), we have $\langle x, \phi \rangle \langle c, \phi \rangle^{-1} \in K$. Immediately, the set $\{\langle x, \phi \rangle \langle c, \phi \rangle^{-1},\ x \in O_M\}$, which will be denoted by $\langle O_M, \phi \rangle \langle c, \phi \rangle^{-1}$, is a fractional ideal of O_K.

It is clear that $\langle c, \phi \rangle^p \in K$. As in (3.1), let us write (in a unique form):

$$\langle c, \phi \rangle^p O_K = \left(I(\phi) \right)^p \prod_{i=1}^{p-1} J_i(\phi)^i.$$

Lemma 4.3. *With the previous notation, we have*: $\langle O_M, \phi \rangle \langle c, \phi \rangle^{-1} = I(\phi)^{-1}$.

Proof. We adapt the proof of Theorem 2.3 in [So1] to our situation (we may also see the proof of Proposition 3.2 in [So6]). Let $\overline{\phi}$ be the complex conjugate character of ϕ. It is easily seen that the elements $\langle x,\phi\rangle\langle y,\overline{\phi}\rangle$ belong to O_K, where x and y are elements of O_M; one denotes by $\langle O_M,\phi\rangle\langle O_M,\overline{\phi}\rangle$ the ideal of O_K generated by all such elements. It follows from [F2, Theorem 18], that

$$\langle O_M,\phi\rangle\langle O_M,\overline{\phi}\rangle = \mathcal{F}(\phi), \tag{4.4}$$

where $\mathcal{F}(\phi)$ is the Artin conductor of ϕ. We let $J(\phi)=\prod_{i=1}^{p-1} J_i(\phi)^i$. For all $x\in O_M$ we have

$$\langle x,\phi\rangle^p O_K = \big(\langle x,\phi\rangle\langle c,\phi\rangle^{-1} I(\phi)\big)^p J(\phi)\subset O_K.$$

But for every prime ideal $\mathfrak{p}$ of O_K, $v_{\mathfrak{p}}(J(\phi))<p$, so that

$$\langle O_M,\phi\rangle\langle c,\phi\rangle^{-1}\subset I(\phi)^{-1}. \tag{4.5}$$

Similarly, as in (3.1) let us write

$$\langle c,\overline{\phi}\rangle^p O_K = \big(I(\overline{\phi})\big)^p \prod_{i=1}^{p-1} J_i(\overline{\phi})^i.$$

We obtain

$$\langle O_M,\overline{\phi}\rangle\langle c,\overline{\phi}\rangle^{-1}\subset I(\overline{\phi})^{-1}. \tag{4.6}$$

On the one hand, by a slight change in numbering, we may write

$$\langle c,\overline{\phi}\rangle^p O_K = \big(I(\overline{\phi})\big)^p \prod_{i=1}^{p-1} J_{p-i}(\overline{\phi})^{p-i}.$$

On the other hand, since $\overline{\phi}=\phi^{p-1}$, we have $\langle c,\overline{\phi}\rangle = d\langle c,\phi\rangle^{p-1}$ with $d\in K$, and using the decomposition of $\langle c,\phi\rangle^p O_K$ we can write

$$\langle c,\overline{\phi}\rangle^p O_K = \left[d\,I(\phi)^{p-1}\prod_{i=1}^{p-1} J_i(\phi)^{i-1}\right]^p \prod_{i=1}^{p-1} J_i(\phi)^{p-i}.$$

Therefore $J_i(\phi)=J_{p-i}(\overline{\phi})$ by the uniqueness of the decomposition of $\langle c,\overline{\phi}\rangle^p O_K$. It follows that

$$\langle c,\phi\rangle\langle c,\overline{\phi}\rangle O_K = I(\phi)I(\overline{\phi})\prod_{i=1}^{p-1} J_i(\phi). \tag{4.7}$$

As $M=K(\langle c,\phi\rangle)$ (ϕ is nontrivial and $\langle c,\phi\rangle\neq 0$), we have $\mathcal{F}(\phi)=\prod_{i=1}^{p-1} J_i(\phi)$ by the second remark which follows Proposition 3.2. From (4.7) and (4.4) we get

$$\langle O_M,\phi\rangle\langle c,\phi\rangle^{-1}\langle O_M,\overline{\phi}\rangle\langle c,\overline{\phi}\rangle^{-1} = I(\phi)^{-1}I(\overline{\phi})^{-1}.$$

It follows, by virtue of (4.5) and (4.6), that

$$\langle O_M, \phi\rangle\langle c, \phi\rangle^{-1} = I(\phi)^{-1}.$$

This completes the proof of the lemma. □

Proof of Proposition 4.2. (i) Obvious.

(ii) Analogous to the proof of Proposition 4.2(ii) in [BGS, p. 24].

(iii) The proof consists in determining the content of the following idele which is defined in Proposition 4.1:

$$h(\chi) = \left(\frac{e(E_{\mathfrak{p}}/k_{\mathfrak{p}})}{e(E/k)} N_{E/k}\left(\frac{\langle b_{\mathfrak{p}}, \psi\rangle_{N/E}}{\langle b, \psi\rangle_{N/E}}\right)\right)_{\mathfrak{p}}.$$

Let $\mathcal{M}_2$ be the maximal O_E-order in $E[V]$. We check easily that

$$E[V] \simeq \prod_{i=0}^{p^r-1} E \quad \text{and} \quad \mathrm{Cl}(\mathcal{M}_2) \simeq \prod_{i=0}^{p^r-1} \mathrm{Cl}(E).$$

Put $\Omega_E = \mathrm{Gal}(\bar{k}/E)$. Let h_2 be the element of $\mathrm{Hom}_{\Omega_E}(R_V, J(\bar{k}))$ which to the trivial character of V assigns 1, and for every nontrivial absolutely irreducible character χ' of V assigns $h_2(\chi')$ defined by: for every prime ideal $\mathfrak{p}$ of O_k, $h_2(\chi')_{\mathfrak{p}} = \frac{\langle b_{\mathfrak{p}}, \chi'\rangle_{N/E}}{\langle b, \chi'\rangle_{N/E}}$. Then h_2 is a representative of $[\mathcal{M}_2 \otimes_{O_E[V]} O_N]$ in the Hom-description of $\mathrm{Cl}(\mathcal{M}_2)$, and the components of $[\mathcal{M}_2 \otimes_{O_E[V]} O_N]$ in $\prod_{i=0}^{p^r-1} \mathrm{Cl}(E)$, identified with $\mathrm{Cl}(\mathcal{M}_2)$, are the classes of the contents of the ideles $h_2(\chi')$.

Let L'/E be the subextension of N/E of degree p fixed by $\mathrm{Ker}(\psi)$. The character ψ factors through a nontrivial character $\underline{\psi}$ of $\mathrm{Gal}(L'/E)$. It is easy to check (as in (4.2) and (4.3)) that we have

$$\frac{\langle b_{\mathfrak{p}}, \psi\rangle_{N/E}}{\langle b, \psi\rangle_{N/E}} = \frac{\langle \mathrm{Tr}_{N_{\mathfrak{p}}/L'_{\mathfrak{p}}}(b_{\mathfrak{p}}), \underline{\psi}\rangle_{L'/E}}{\langle \mathrm{Tr}_{N/L'}(b), \underline{\psi}\rangle_{L'/E}}.$$

It follows from [F4, Note 4, pp. 50–51] that the class in $\mathrm{Cl}(E)$ of the content of the idele whose components occur on the right-hand side of the preceding equality is the class of the following fractional ideal:

$$\langle O_{L'}, \underline{\psi}\rangle_{L'/E}\langle \mathrm{Tr}_{N/L'}(b), \underline{\psi}\rangle_{L'/E}^{-1}.$$

Let us calculate the class of this fractional ideal. We let $c = \mathrm{Tr}_{N/L'}(b)$. Recall that c is a normal basis of L'/E, and then $L' = E(\langle c, \underline{\psi}\rangle_{L'/E})$. One knows that there exists i_0, $0 \leqslant i_0 \leqslant p^r - 2$, such that $\sigma^{i_0}(L) = L'$ (recall that $L = E(\sqrt[p]{\hat{g}(\sigma)m})/E$ is a subextension of N/E of degree p); consequently $L' = E(\sqrt[p]{\sigma^{i_0}\hat{g}(\sigma)m})/E$. By Kummer theory, there exist $e \in E$ and $1 \leqslant v \leqslant p-1$ such that

$$\big(\langle c, \underline{\psi}\rangle_{L'/E}\big)^p = e^p\big(v\sigma^{i_0}\hat{g}(\sigma)\big)m.$$

Clearly the image $\overline{v\sigma^{i_0}\hat{g}(\sigma)}$ in $\mathbb{F}_p[C]$ is a nonzero codeword of the cyclic code $(\hat{g}(\sigma))$. Then there exist $q(\sigma) \in \mathbb{Z}[C]$ and $0 \leqslant j \leqslant p^r - 2$ such that $v\sigma^{i_0}\hat{g}(\sigma) = pq(\sigma) + \sigma^j\hat{g}(\sigma)$ (recall that $(\hat{g}(\sigma))$ consists of 0 and the cyclic shifts of $\hat{g}(\sigma)$; see the proof of Proposition 2.6). One deduces that the decomposition of $(\langle c, \underline{\psi}\rangle_{L'/E})^p O_E$ as in (3.1) is the following:

$$\big(\langle c, \underline{\psi}\rangle_{L'/E}\big)^p O_E = \big[e\big(q(\sigma)m\big)\sigma^j\big(I\big(\hat{g}(\sigma)m\big)\big)\big]^p \prod_{i=1}^{p-1}\big[\sigma^j(J_i)\big]^i.$$

Lemma 4.3 gives us

$$\langle O_{L'}, \underline{\psi}\rangle_{L'/E}\langle c, \underline{\psi}\rangle_{L'/E}^{-1} = \big[e\big(q(\sigma)m\big)\sigma^j\big(I\big(\hat{g}(\sigma)m\big)\big)\big]^{-1}.$$

Therefore

$$\mathrm{cl}\big(\langle O_{L'}, \underline{\psi}\rangle_{L'/E}\langle \mathrm{Tr}_{N/L'}(b), \underline{\psi}\rangle_{L'/E}^{-1}\big) = \sigma^j\big(\mathrm{cl}\big(I\big(\hat{g}(\sigma)m\big)\big)^{-1}\big). \tag{4.8}$$

Let I be the ideal of O_k which is the content of the idele $(\frac{e(E_\mathfrak{p}/k_\mathfrak{p})}{e(E/k)})_\mathfrak{p}$. Since $(e(E_\mathfrak{p}/k_\mathfrak{p}))^2 O_{k,\mathfrak{p}}$ is equal to the local discriminant $\Delta(E_\mathfrak{p}/k_\mathfrak{p})$, we have

$$I^2 = \frac{\Delta(E/k)}{e(E/k)^2}.$$

As $d = e(E/k)^2$ is the discriminant of a basis of E/k, we have $\mathrm{cl}_k(O_E) = \mathrm{cl}(\sqrt{\Delta(E/k)/d})$ by Artin's theorem (see Proposition 3.1). One deduces that $\mathrm{cl}_k(O_E) = \mathrm{cl}(I)$. From this last equality and (4.8) we obtain: the class in $\mathrm{Cl}(k)$ of the content of the idele $h(\chi)$ is $\mathrm{cl}_k(O_E)N_{E/k}(\sigma^j(\mathrm{cl}(I(\hat{g}(\sigma)m))^{-1}))$, which is equal to $\mathrm{cl}_k(O_E)N_{E/k}(\mathrm{cl}(I(\hat{g}(\sigma)m))^{-1})$. This completes the proof of (iii). □

Proposition 4.4. *Let $\mathfrak{P}$ be a prime ideal of O_E. Then, for every $e(\sigma) \in \mathbb{Z}[C]$, the integral weight of the p-part of $\mathfrak{P}^{e(\sigma)\hat{g}(\sigma)}$ is divisible by $p^{r-1}(p-1)/2$, where $\hat{g}(\sigma)$ is considered as an element of $\mathbb{N}[C]$.*

Proof. We will distinguish two cases, depending on whether $\mathfrak{P} \cap O_k$ is totally split in E/k or not.

(1) Assume that $\mathfrak{P} \cap O_k$ is not totally split in E/k. We have seen, in the proof of the assertion (1) of Proposition 3.5, that $\mathfrak{P}^{e(\sigma)\hat{g}(\sigma)}$ is a pth power of an ideal of O_E. Therefore the integral weight of its p-part is $w_{\mathrm{in}}(e(\sigma)\hat{g}(\sigma))/p = e(1)\hat{g}(1)/p$. We conclude thanks to the part of Proposition 2.6 which says $\hat{g}(1) = p^r(p-1)/2$ $(= w_{\mathrm{in}}(\hat{g}(\sigma)))$.

(2) Assume now that $\mathfrak{P} \cap O_k$ is totally split in E/k. Put $\alpha(\sigma) = e(\sigma)\hat{g}(\sigma)$. Clearly we may write $\alpha(\sigma) = pq(\sigma) + r(\sigma)$, where the coefficients in the basis C of $r(\sigma)$ belong to $\{0, 1, \ldots, p-1\}$. As $\mathfrak{P}^{\alpha(\sigma)} = (\mathfrak{P}^{q(\sigma)})^p\mathfrak{P}^{r(\sigma)}$ and $\mathfrak{P} \cap O_k$ is totally split in E/k, the p-part of $\mathfrak{P}^{\alpha(\sigma)}$ is $\mathfrak{P}^{q(\sigma)}$, and then its integral weight is $w_{\mathrm{in}}(q(\sigma)) = [w_{\mathrm{in}}(\alpha(\sigma)) - w_{\mathrm{in}}(r(\sigma))]/p$. On the one hand, $w_{\mathrm{in}}(\alpha(\sigma)) = e(1)\hat{g}(1)$. On the other hand, the image $\overline{\alpha(\sigma)} = \overline{r(\sigma)}$ in $\mathbb{F}_p[C]$ is a codeword of the code of $\mathbb{F}_p[C]$ generated by $\hat{g}(\sigma)$. By Proposition 2.6, it follows that $w_{\mathrm{in}}(r(\sigma)) = w_{\mathrm{in}}(\hat{g}(\sigma)) = \hat{g}(1)$ or 0 depending on whether $r(\sigma) \neq 0$ or not. Thus $w_{\mathrm{in}}(q(\sigma)) = \hat{g}(1)(e(1)-1)/p$ or $\hat{g}(1)e(1)/p$. We complete the proof by replacing $\hat{g}(1)$ by its value. □

Proof of Theorem 1.1. Proposition 4.2 allows us to identify $\mathcal{R}(\mathcal{M})$ with a subset of $\prod_{i=1}^{n} \mathrm{Cl}(k(\chi_i)) \times \mathrm{Cl}(k)$. In the following discussion we will prove the inclusions: $\mathcal{R}(\mathcal{M}) \subset A$ and $A \subset \mathcal{R}(\mathcal{M})$, where A is the set defined in the statement of Theorem 1.1.

(1) Let us show the inclusion $\mathcal{R}(\mathcal{M}) \subset A$.

One uses the hypotheses and notation of Proposition 4.2. First

$$(c_1, c_2, \ldots, c_n) \in \mathcal{R}\big(\mathcal{M}(C)\big)$$

by that proposition. Arguing as in part (1) of the proof of [BGS, Theorem 1.1, p. 25], we obtain

$$\mathrm{cl}_k(O_E) = \prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i)^{\chi_i(1)} = \prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i). \tag{4.9}$$

As in the beginning of the proof of the inclusion (3.2) (see Section 3), let us write

$$m O_E = \prod_{i=1}^{s} \mathfrak{P}_i^{e_i(\sigma)},$$

where $s \geqslant 1$, the $e_i(\sigma) \in \mathbb{Z}[C]$, and the $\mathfrak{P}_i$ are prime ideals of O_E above distinct prime ideals of O_k. Then

$$\hat{g}(\sigma) m O_E = \prod_{i=1}^{s} \mathfrak{P}_i^{e_i(\sigma)\hat{g}(\sigma)}.$$

For every i, $1 \leqslant i \leqslant s$, there exist $q_i(\sigma), r_i(\sigma) \in \mathbb{Z}[C]$ such that

$$\mathfrak{P}_i^{e_i(\sigma)\hat{g}(\sigma)} = \big(\mathfrak{P}_i^{q_i(\sigma)}\big)^p \mathfrak{P}_i^{r_i(\sigma)},$$

where $\mathfrak{P}_i^{q_i(\sigma)}$ is the p-part of $\mathfrak{P}_i^{e_i(\sigma)\hat{g}(\sigma)}$, and for every prime ideal $\mathfrak{P}$ of O_E, $0 \leqslant v_{\mathfrak{P}}(\mathfrak{P}_i^{r_i(\sigma)}) < p$. Since the $\mathfrak{P}_i^{r_i(\sigma)}$ are pairwise relatively prime, we deduce that the p-part of $\hat{g}(\sigma) m O_E$ is

$$I\big(\hat{g}(\sigma) m\big) = \prod_{i=1}^{s} \mathfrak{P}_i^{q_i(\sigma)}.$$

Therefore

$$N_{E/k}\big(I\big(\hat{g}(\sigma) m\big)\big) = \prod_{i=1}^{s} N_{E/k}(\mathfrak{P}_i)^{w_{\mathrm{in}}(\mathfrak{P}_i^{q_i(\sigma)})}.$$

By Proposition 4.4, $w_{\mathrm{in}}(\mathfrak{P}_i^{q_i(\sigma)})$ is divisible by $p^{r-1}(p-1)/2$. Consequently

$$N_{E/k}\big(I\big(\hat{g}(\sigma) m\big)\big) = N_{E/k}\big(I'\big(\hat{g}(\sigma) m\big)\big)^{p^{r-1}(p-1)/2},$$

where $I'(\hat{g}(\sigma)m)$ is a fractional ideal of O_E. One deduces the existence of $c \in \mathrm{Cl}(E)$ satisfying

$$N_{E/k}\big(\mathrm{cl}\big(I\big(\hat{g}(\sigma)m\big)^{-1}\big)\big) = N_{E/k}(c)^{p^{r-1}(p-1)/2}. \tag{4.10}$$

From Proposition 4.2(iii), (4.9) and (4.10) we get

$$c_{n+1} = \left(\prod_{i=1}^{n} N_{k(\chi_i)/k}(c_i)\right)\big(N_{E/k}(c)\big)^{p^{r-1}(p-1)/2}.$$

We conclude that $(c_1, c_2, \ldots, c_{n+1}) \in A$. Hence $\mathcal{R}(\mathcal{M}) \subset A$.

(2) Let us show the inclusion $A \subset \mathcal{R}(\mathcal{M})$.

Let $X = (x_1, x_2, \ldots, x_n, x_{n+1} = x\prod_{i=1}^{n} N_{k(\chi_i)/k}(x_i)) \in A$, where x is an element of $\mathrm{Cl}(k)^{p^{r-1}(p-1)/2}$. First we consider the element $(x_1, x_2, \ldots, x_n)$ of $\mathcal{R}(\mathcal{M}(C))$. Let $\mathrm{Ex}\colon \mathrm{Cl}(O_k[C]) \to \mathrm{Cl}(\mathcal{M}(C))$ be the surjection induced by extension of scalars from $O_k[C]$ to $\mathcal{M}(C)$. Since $Ex(\mathcal{R}(O_k[C])) = \mathcal{R}(\mathcal{M}(C))$, the assertions (a), (b) of [M3, Theorem 6.17, p. 289], guarantee the existence of a tame Galois extension E/k with Galois group isomorphic to C, such that $[\mathcal{M}(C) \otimes_{O_k[C]} O_E] = (x_1, x_2, \ldots, x_n)$ and the only subextension of E/k unramified over k is k itself. This last fact implies that $N_{E/k}\colon \mathrm{Cl}(E) \to \mathrm{Cl}(k)$ is surjective thanks to [W, Theorem 10.1, p. 400].

Next we consider the element x of $\mathrm{Cl}(k)^{p^{r-1}(p-1)/2}$. Let $y \in \mathrm{Cl}(k)$ be such that $x = y^{p^{r-1}(p-1)/2}$. Choose $c \in \mathrm{Cl}(E)$ such that $N_{E/k}(c) = y$.

By the Tchebotarev density theorem, there exists a prime ideal $\mathfrak{P}$ of O_E, totally split in E/k, relatively prime to $(1-\xi_p)^p O_E$ and such that $c^{-1} = \mathrm{cl}(\mathfrak{P})$. Let us consider now $\mathrm{cl}(\mathfrak{P}^2)^{-1}$. Recall that $\mathrm{Cl}(E, (1-\xi_p)^p O_E)$ is the ray class group modulo $(1-\xi_p)^p O_E$. By the canonical surjection from $\mathrm{Cl}(E, (1-\xi_p)^p O_E)$ to $\mathrm{Cl}(E)$ and the Tchebotarev density theorem, there exists a prime ideal $\mathfrak{Q}$ of O_E, relatively prime to $(1-\xi_p)^p O_E$ and to all the conjugates of $\mathfrak{P}$ under $\mathrm{Gal}(E/k)$, such that $\mathfrak{Q} \cap O_k$ is totally split in E/k and $\mathrm{cl}(\mathfrak{P}^2)^{-1} = \mathrm{cl}(\mathfrak{Q})$ in $\mathrm{Cl}(E, (1-\xi_p)^p O_E)$. Consequently, there exists $m \in E^\times$ such that

$$m O_E = \mathfrak{P}^2\mathfrak{Q} \quad \text{and} \quad m \equiv 1 \mod^* (1-\xi_p)^p O_E.$$

Consider now $\hat{g}(\sigma)$ as an element of $\mathbb{N}[C]$. We have the equality

$$\hat{g}(\sigma) m O_E = \mathfrak{P}^{2\hat{g}(\sigma)}\mathfrak{Q}^{\hat{g}(\sigma)}.$$

One considers the extension $L = E(\sqrt[p]{\hat{g}(\sigma)m})/E$. As in the proof of the inclusion (3.4) (see Section 3), we check without difficulty that L/E is tame of degree p, and its Galois closure is a tame extension N/k with Galois group isomorphic to Γ.

Since $\mathfrak{Q}$ is totally split in E/k and relatively prime to the conjugates of $\mathfrak{P}$, and since the coefficients of $\hat{g}(\sigma)$ belong to $\{0, 1, \ldots, p-1\}$, we have that the p-part $I(\hat{g}(\sigma)m)$ of $\hat{g}(\sigma)m O_E$ is equal to that of $\mathfrak{P}^{2\hat{g}(\sigma)}$.

The ideal $\mathfrak{P} \cap O_k$ of O_E being totally split in E/k, in order to calculate the exact value of $w_{\mathrm{in}}(I(\hat{g}(\sigma)m))$, let us follow the part (2) of the proof of Proposition 4.4. We write $2\hat{g}(\sigma) = pq(\sigma) + r(\sigma)$, where the coefficients in the basis C of $r(\sigma)$ belong to $\{0, 1, \ldots, p-1\}$. Then

$$\mathfrak{P}^{2\hat{g}(\sigma)} = \big(\mathfrak{P}^{q(\sigma)}\big)^p \mathfrak{P}^{r(\sigma)}, \quad I\big(\hat{g}(\sigma)m\big) = \mathfrak{P}^{q(\sigma)},$$

and

$$w_{\text{in}}\big(I\big(\hat{g}(\sigma)m\big)\big) = w_{\text{in}}\big(q(\sigma)\big) = \big[w_{\text{in}}\big(2\hat{g}(\sigma)\big) - w_{\text{in}}\big(r(\sigma)\big)\big]/p.$$

Clearly $r(\sigma) \neq 0$ (p is odd), whence $w_{\text{in}}(r(\sigma)) = \hat{g}(1)$, and then

$$w_{\text{in}}\big(I\big(\hat{g}(\sigma)m\big)\big) = \big[2\hat{g}(1) - \hat{g}(1)\big]/p = \hat{g}(1)/p.$$

Since $\hat{g}(1) = p^r(p-1)/2$ (see Proposition 2.6), $w_{\text{in}}(I(\hat{g}(\sigma)m)) = p^{r-1}(p-1)/2$. It follows that

$$\begin{aligned} N_{E/k}\big(\text{cl}\big(I\big(\hat{g}(\sigma)m\big)^{-1}\big)\big) &= N_{E/k}\big(\text{cl}(\mathfrak{P})^{-1}\big)^{p^{r-1}(p-1)/2} \\ &= N_{E/k}(c)^{p^{r-1}(p-1)/2} = y^{p^{r-1}(p-1)/2} = x. \end{aligned}$$

As in (4.9), we have $\text{cl}_k(O_E) = \prod_{i=1}^{n} N_{k(\chi_i)/k}(x_i)$. Then, by virtue of Proposition 4.2, $[\mathcal{M} \otimes_{O_k[\Gamma]} O_N] = X$. Therefore $X \in \mathcal{R}(\mathcal{M})$, whence $A \subset \mathcal{R}(\mathcal{M})$. □

Proof of Corollary 1.2. We have seen in Section 2 (see Remark (2) following Proposition 2.3) that the symmetric group S_3 is an example of a group Γ satisfying the hypotheses of Theorem 1.1; in this case C (respectively V) is a cyclic group of order 2 (respectively 3). If $\xi_3 = j \in k$, by Theorem 1.1 we have $\mathcal{R}(\mathcal{M}) = \{(c, xc) \mid c \in \text{Cl}(k),\ x \in \text{Cl}(k)\}$; immediately this last set is equal to $\text{Cl}(k) \times \text{Cl}(k)$. If $j \notin k$, then k is linearly disjoint from $\mathbb{Q}(j)$ over $\mathbb{Q}$. It follows from [So2] (case $\ell = 3$, $q = 2$) and [BS2, Appendix], that: $k[S_3] \simeq k \times k \times M_2(k)$, $\text{Cl}(\mathcal{M}) \simeq \text{Cl}(k) \times \text{Cl}(k) \times \text{Cl}(k)$, and $\mathcal{R}(\mathcal{M}) = \{(c, xc) \mid c \in \text{Cl}(k),\ x \in \text{Cl}(k)\}$; to check these assertions, it suffices to see, in the notation of [So2], that $K = k$ and the Stickelberger ideals $\mathcal{S}_2$ and $\mathcal{S}_3$ are respectively equal to $\mathbb{Z}$ and $\mathbb{Z}[\text{Gal}(k(j)/k)]$. □

References

[A] E. Artin, Questions de base minimale dans la théorie des nombres algébriques, in: Algèbre et Théorie des Nombres, in: Colloq. Internat. CNRS, vol. 24, CNRS, Paris, 1950, pp. 19–20.

[BGS] N.P. Byott, C. Greither, B. Sodaïgui, Classes réalisables d'extensions non abéliennes, J. Reine Angew. Math. 601 (2006) 1–27.

[BS1] N.P. Byott, B. Sodaïgui, Realizable Galois module classes for tetrahedral extensions, Compos. Math. 141 (2005) 573–582.

[BS2] N.P. Byott, B. Sodaïgui, Galois module structure for dihedral extensions of degree 8: Realizable classes over the group ring, J. Number Theory 112 (2005) 1–19.

[C] J.E. Carter, Steinitz classes of nonabelian extensions of degree p^3, Acta Arith. 78 (1997) 297–303.

[Co1] H. Cohen, A Course in Computational Algebraic Number Theory, Grad. Texts in Math., vol. 138, Springer-Verlag, New York, 1995.

[Co2] H. Cohen, Advanced Topics in Computational Number Theory, Grad. Texts in Math., vol. 193, Springer-Verlag, New York, 2000.

[CR1] C.W. Curtis, I. Reiner, Methods of Representation Theory with Applications to Finite Groups and Orders, vol. I, Wiley–Interscience, New York, 1981.

[CR2] C.W. Curtis, I. Reiner, Methods of Representation Theory with Applications to Finite Groups and Orders, vol. II, Wiley–Interscience, New York, 1987.

[F1] A. Fröhlich, The discriminant of relative extensions and the existence of integral bases, Mathematika 7 (1960) 15–22.

[F2] A. Fröhlich, Arithmetic and Galois module structure for tame extensions, J. Reine Angew. Math. 286/287 (1976) 380–440.

[F3] A. Fröhlich, Galois module structure, in: Algebraic Number Fields, Proceedings of the Durham Symposium, 1975, Academic Press, London, 1977, pp. 133–191.
[F4] A. Fröhlich, Galois Module Structure of Algebraic Integers, Springer-Verlag, Berlin, 1983.
[FT] A. Fröhlich, M.J. Taylor, Algebraic Number Theory, Cambridge Univ. Press, 1991.
[GS1] M. Godin, B. Sodaïgui, Classes de Steinitz d'extensions à groupe de Galois A_4, J. Théor. Nombres Bordeaux 14 (2002) 241–248.
[GS2] M. Godin, B. Sodaïgui, Realizable classes of tetrahedral extensions, J. Number Theory 98 (2003) 320–328.
[GS3] M. Godin, B. Sodaïgui, Module structure of rings of integers in octahedral extensions, Acta Arith. 109.4 (2003) 321–327.
[H] E. Hecke, Lectures on the Theory of Algebraic Numbers, Grad. Texts in Math., vol. 77, Springer-Verlag, New York, 1981.
[LN] R. Lidl, H. Niederreiter, Finite Fields, second ed., Encyclopedia Math. Appl., vol. 20, Cambridge Univ. Press, 1997.
[M1] L.R. McCulloh, Cyclic extensions without integral bases, Proc. Amer. Math. Soc. 17 (1966) 1191–1194.
[M2] L.R. McCulloh, Galois module structure of elementary abelian extensions, J. Algebra 82 (1983) 102–134.
[M3] L.R. McCulloh, Galois module structure of abelian extensions, J. Reine Angew. Math. 375/376 (1987) 259–306.
[N] J. Neukirch, Class Field Theory, Springer-Verlag, Berlin, 1986.
[R] I. Reiner, Maximal Orders, Academic Press, 1975.
[Ro] S. Roman, Coding and Information Theory, Grad. Texts in Math., vol. 134, Springer-Verlag, New York, 1992.
[Se1] J.-P. Serre, Linear Representations of Finite Groups, third ed., Grad. Texts in Math., vol. 42, Springer-Verlag, New York, 1986.
[Se2] J.-P. Serre, Local Fields, second ed., Grad. Texts in Math., vol. 67, Springer-Verlag, New York, 1995.
[So1] B. Sodaïgui, Structure galoisienne relative des anneaux d'entiers, J. Number Theory 28 (2) (1988) 189–204.
[So2] B. Sodaïgui, Classes réalisables par des extensions métacycliques non abéliennes et éléments de Stickelberger, J. Number Theory 65 (1997) 87–95.
[So3] B. Sodaïgui, Classes de Steinitz d'extensions galoisiennes relatives de degré une puissance de 2 et problème de plongement, Illinois J. Math. 43 (1) (1999) 47–60.
[So4] B. Sodaïgui, "Galois module structure" des extensions quaternioniennes de degré 8, J. Algebra 213 (1999) 549–556.
[So5] B. Sodaïgui, Relative Galois module structure and Steinitz classes of dihedral extensions of degree 8, J. Algebra 223 (2000) 367–378.
[So6] B. Sodaïgui, Realizable classes of quaternion extensions of degree 4l, J. Number Theory 80 (2000) 304–315.
[Sov] E. Soverchia, Steinitz classes of metacyclic extensions, J. London Math. Soc. (2) 66 (1) (2002) 61–72.
[Sw] R.G. Swan, Projective modules over group rings and maximal orders, Ann. of Math. (2) 76 (1962) 55–61.
[T] M.J. Taylor, On Fröhlich's conjecture for rings of tame extensions, Invent. Math. 63 (1981) 41–79.
[W] L.C. Washington, Introduction to Cyclotomic Fields, second ed., Springer-Verlag, Berlin, 1996.